AVG 9 Internet Security

Gebruikershandleiding

Documentrevisie 90.21 (3.2.2010)

Inhoud

1. Inleiding

Deze gebruikershandleiding bevat uitgebreide informatie over **AVG 9 Internet Security** .

Gefeliciteerd met uw aankoop van AVG 9 Internet Security!

AVG 9 Internet Security is één van een reeks onderscheiden AVG producten die zijn ontwikkeld om uw gemoedsrust te bevorderen en uw pc volledig te beschermen. Net als alle AVG producten is **AVG 9 Internet Security** volledig opnieuw ontwikkeld, om u de gerenommeerde en erkende AVG-beveiliging te kunnen bieden, op een nieuwe, efficiëntere en meer gebruikersvriendelijke manier.

Uw nieuwe **AVG 9 Internet Security** beschikt over een gestroomlijnde gebruikersinterface, gecombineerd met een agressievere en snellere scanfunctie. Om het u gemakkelijk te maken zijn meer beveiligingsfuncties geautomatiseerd, en zijn nieuwe, 'intelligente' gebruikersopties toegevoegd, zodat u onze beveiligingsfuncties aan uw wensen kunt aanpassen. Geen compromissen meer tussen veiligheid en gemak!

AVG is ontwikkeld om de omgeving waarin uw computer en netwerk moeten functioneren, te beschermen. Geniet van de volledige bescherming van AVG.

2. AVG installatievereisten

2.1. Ondersteunde besturingssystemen

AVG 9 Internet Securityis ontworpen om werkstations met de volgende besturingssystemen te beschermen:

- Windows 2000 Professional SP4 + Update Rollup 1
- Windows XP Home Edition SP2
- Windows XP Professional SP2
- Windows XP Professional x64 Edition SP1
- Windows Vista (x86 en x64, alle edities)
- Windows 7 (x86 en x64, alle edities)

(en mogelijk hogere servicepacks voor bepaalde besturingssystemen)

***Opmerking**: het onderdeel Identity Protection wordt niet ondersteund onder Windows 2000 en XP x64. U kunt %main_product_name_in_text%> op deze besturingssystemen installeren, maar dan zonder het onderdeel IDP.*

2.2. Minimale en aanbevolen hardwarevereisten

Minimale hardwarevereisten voor **AVG 9 Internet Security**:

- Intel Pentium CPU 1,5 GHz
- 512 MB RAM-geheugen
- 390 MB vrije schijfruimte (voor de installatie)

Aanbevolen hardwarevereisten voor **AVG 9 Internet Security**:

- Intel Pentium CPU 1,8 GHz
- 512 MB RAM-geheugen

- 510 MB vrije schijfruimte (voor de installatie)

3. AVG installatieopties

AVG kan geïnstalleerd worden met het installatiebestand op uw installatie-cd. U kunt het nieuwste installatiebestand echter ook downloaden vanaf de website van AVG (http://www.avg.com/).

Voordat u AVG installeert, raden wij u nadrukkelijk aan de website van AVG(http://www.avg.com/) te bezoeken om na te gaan of er een nieuw installatiebestand is. Zo bent u er zeker van dat u de meest recente versie van AVG 9 Internet Security installeert.

Wij adviseren u om ons nieuwe hulpmiddel AVG Download Manager uit te proberen. Dit helpt u om het installatiebestand in uw taal in te stellen!

Tijdens het installatieproces wordt u om uw licentie/verkoop-nummer gevraagd. Zorg ervoor dat u het bij de hand hebt voordat u met de installatie begint. Het verkoopnummer staat op de cd-hoes. Als u uw exemplaar van AVG online hebt aangeschaft, hebt u het licentienummer per e-mail ontvangen.

4. AVG Download Manager

AVG Download Manager is een eenvoudig te gebruiken hulpmiddel dat u helpt het juiste installatiebestand te selecteren voor de proefversie van uw AVG-product. Op basis van de door u ingevoerde gegevens selecteert de manager een specifiek product, licentietype en een taal. Tot slot begint **AVG Download Manager** met downloaden en wordt de juiste installatieprocedure gestart.

Waarschuwing: *AVG Download Manager is niet bedoeld voor het downloaden van netwerk- en MKB-edities en alleen de volgende besturingssystemen worden ondersteund: Windows 2000 (SP4 en SRP-rollup), Windows XP, Windows Vista en Windows 7.*

AVG Download Manager kan worden gedownload van de AVG-website (http://www.avg.com/). Hieronder volgt een korte beschrijving van de stappen die u uitvoert in de **AVG Download Manager:**

4.1. Taalselectie

In deze eerste stap van **AVG Download Manager** selecteert u de taal voor de installatieprocedure in de vervolgkeuzelijst. Let wel, deze keuze geldt alleen voor de installatieprocedure; na de installatie krijgt u de gelegenheid om in het programma de instellingen voor taal te wijzigen. Klik vervolgens op de knop ***Volgende*** om door te gaan.

4.2. Verbindingscontrole

In deze stap probeert **AVG Download Manager** een verbinding tot stand te brengen via internet om te zoeken naar updates. U kunt de downloadprocedure pas voortzetten als **AVG Download Manager** de verbindingscontrole tot een goed einde heeft gebracht.

- Als de test geen verbinding oplevert, controleert u of u bent aangesloten op internet. Klik vervolgens op de knop ***Opnieuw***

- Als u voor de verbinding met internet gebruikmaakt van een proxyserver, klikt u op de knop ***Proxy-instellingen*** om proxyserverinstellingen op te geven:

- Als de controle succesvol is verlopen, klikt u op de knop ***Volgende*** om door te gaan.

4.3. Proxy-instellingen

Als **AVG Download Manager** er niet in is geslaagd uw proxy-instellingen te achterhalen, zult u deze handmatig moeten opgeven. Geef de volgende instellingen op:

- ***Server*** - voer een geldige naam voor de proxyserver of een geldig IP-adres in
- ***Poort*** - voer het bijbehorende poortnummer in
- ***Proxy-verificatie gebruiken*** - als voor de proxyserver verificatie is vereist, schakelt u dit selectievakje in.
- ***Verificatietype selecteren*** - selecteer in het vervolgkeuzemenu het verificatietype. We raden u met nadruk aan de standaardwaarde te handhaven (*de proxyserver geeft dan automatisch aan u door welke eisen aan de verbinding worden gesteld*). Gevorderde gebruikers kunnen ook kiezen voor Basis (*voor sommige servers vereist*) of NTLM (*vereist voor alle ISA-servers*). Voer vervolgens een geldige ***Gebruikersnaam*** en een geldig ***Wachtwoord*** in (optioneel).

Klik op de knop ***Toepassen*** om uw instellingen te bevestigen en om door te gaan naar de volgende stap van **AVG Download Manager**.

4.4. Bestanden voor installatie downloaden

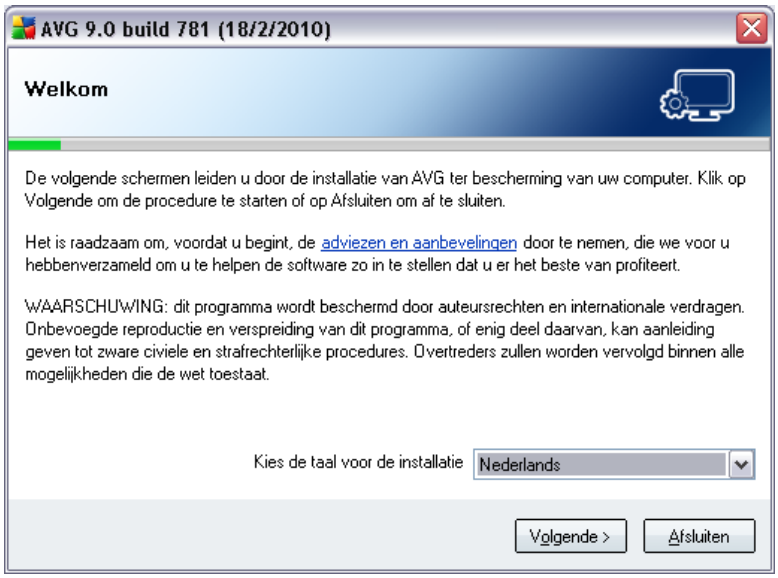
U hebt nu alle informatie opgegeven die **AVG Download Manager** nodig heeft om het downloaden van het installatiepakket te starten en daarna met de installatie te beginnen. Ga door naar de installatieprocedure van AVG.

5. AVG installatieprocedure

Als u **AVG 9 Internet Security** op uw computer wilt installeren, moet u over het meest recente installatiebestand beschikken. U kunt het installatiebestand gebruiken dat op de cd staat die onderdeel uitmaakt van de editie in de doos, maar dat bestand kan verouderd zijn. We raden u daarom aan het nieuwste installatiebestand online op te vragen. U kunt dit downloaden van de AVG-website (http://www.avg.com/), vanaf de pagina ***Ondersteuningscentrum / Downloads***. U kunt nu ook gebruikmaken van ons nieuwe hulpprogramma ***AVG Download Manager*** dat u helpt bij het samenstellen en downloaden van het pakket bestanden dat u voor installatie nodig hebt, en vervolgens de installatie op gang brengt.

De installatieprocedure bestaat uit een reeks dialoogvensters met steeds een korte beschrijving bij elke stap. Hieronder volgt een toelichting op de dialoogvensters:

5.1. Start van installatie

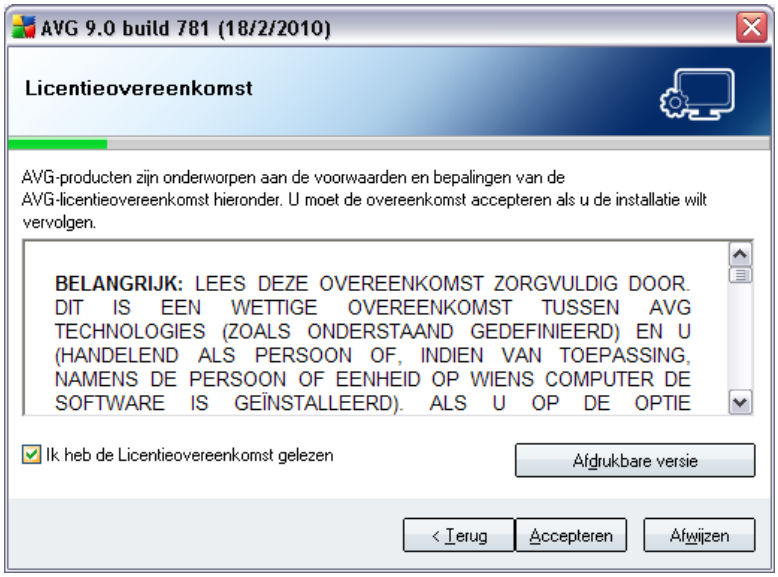


De installatieprocedure begint met het venster ***Welkom bij het installatieprogramma***. In dat venster kiest u de taal die u wilt gebruiken voor de installatieprocedure. In het onderste deel van het venster staat de optie ***Kies uw taal voor de installatie***; daar selecteert u de gewenste taal in het vervolgkeuzemenu. Klik daarna op de knop ***Volgende*** om de keuze te bevestigen en verder te gaan naar het volgende dialoogvenster.

Let op: *u selecteert hier alleen een taal voor de installatieprocedure. U kiest nog geen taal voor de AVG toepassing zelf - dat gebeurt in een later stadium van de*

installatieprocedure!

5.2. Licentieovereenkomst



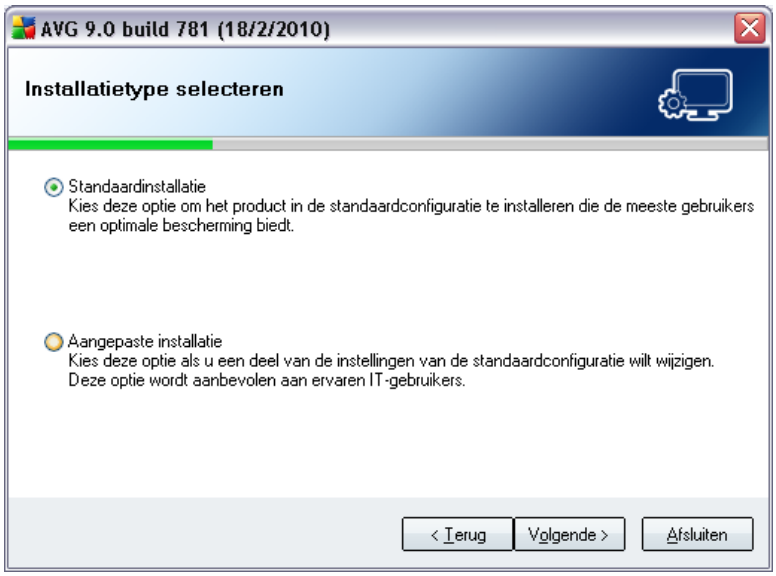
In het dialoogvenster ***Licentieovereenkomst*** staat de volledige tekst van de AVG Licentieovereenkomst. Neem die zorgvuldig door en bevestig dat u de overeenkomst hebt gelezen, begrepen en geaccepteerd door het selectievakje ***Ik heb de licentieovereenkomst gelezen*** in te schakelen en op de knop ***Accepteren*** te klikken.

Als u niet instemt met de licentieverklaring, klikt u op de knop ***Afwijzen***, dan wordt de installatieprocedure meteen afgebroken.

5.3. Systeemstatus controleren

Nadat u zich akkoord hebt verklaard met de licentieverklaring, wordt u omgeleid naar het dialoogvenster ***Systeemstatus controleren***. U hoeft in dit dialoogvenster niets te doen; uw systeem wordt gecontroleerd voordat u kunt beginnen met de installatie van AVG. Wacht tot het proces is voltooid, daarna wordt automatisch het volgende dialoogvenster geopend.

5.4. Installatietype selecteren



In het dialoogvenster ***Installatietype selecteren*** kunt u kiezen uit twee typen installatie: ***standaard*** en ***aangepaste*** installatie.

We raden de meeste gebruikers aan de ***standaardinstallatie*** te gebruiken, waarbij AVG in een automatische modus wordt geïnstalleerd met vooraf door de leverancier ingestelde instellingen. Die configuratie combineert maximale bescherming met een efficiënt gebruik van o.a. werkgeheugen. Als het in de toekomst nodig mocht blijken om de configuratie aan te passen, kunt u dat altijd vanuit de AVG toepassing doen.

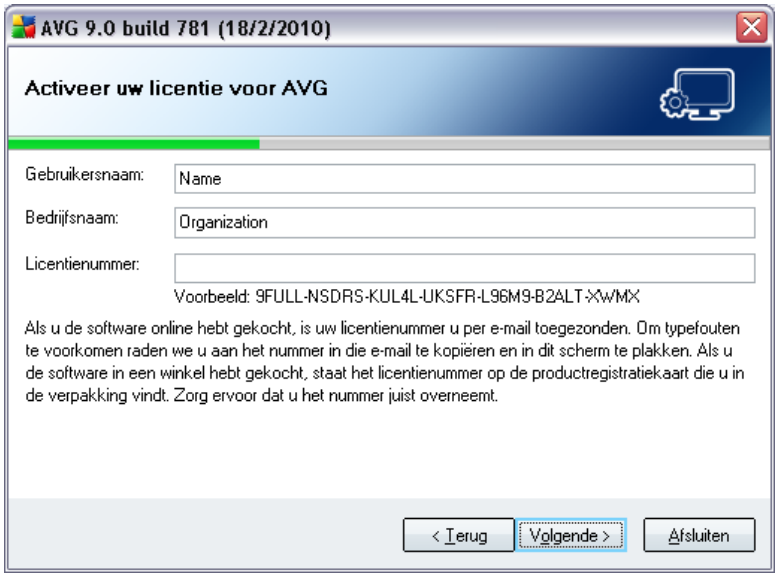
Een aangepaste installatie is alleen aanbevolen voor ervaren gebruikers die een goede reden hebben om AVG te installeren met afwijkende instellingen, bijvoorbeeld om te voldoen aan specifieke systeemvereisten.

5.5. Uw AVG-licentie activeren

In het dialoogvenster ***Uw AVG-licentie activeren*** vult u uw registratiegegevens in. Typ uw naam (in het veld ***Gebruikersnaam***) en de naam van uw organisatie (in het veld ***Bedrijfsnaam***).

Voer vervolgens uw licentienummer/verkoopnummer in in het veld ***Licentienummer***. Het verkoopnummer vindt u op de cd-verpakking in de doos voor **AVG 9 Internet Security**. Het licentienummer staat in de bevestiging die u via e-mail hebt ontvangen na aankoop van **AVG 9 Internet Security** online. U moet dat nummer precies zo typen

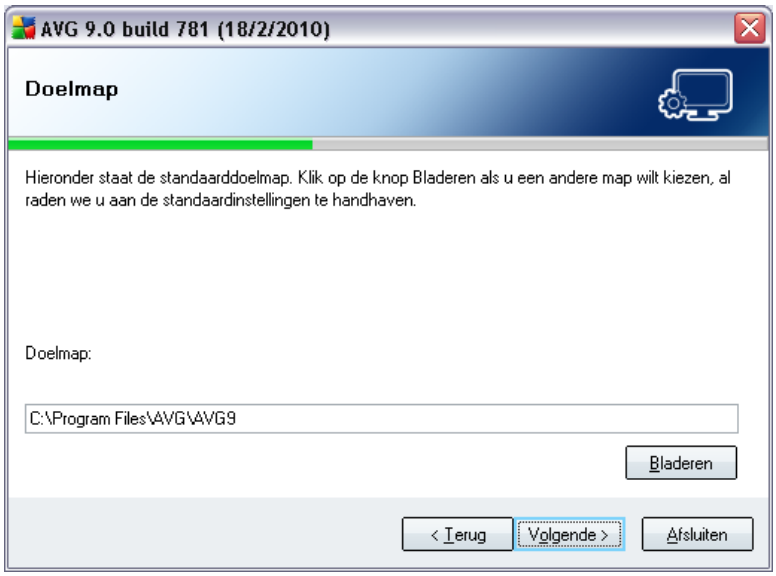
als het wordt weergegeven. Als u beschikt over de digitale versie van het licentienummer (*in de e-mail*), is het raadzaam het nummer over te nemen met kopiëren-en-plakken.



Klik op de knop ***Volgende*** om verder te gaan met de installatieprocedure.

Als u bij de vorige stap hebt gekozen voor een standaardinstallatie, wordt meteen het dialoogvenster ***AVG Werkbalk Beveiliging* geopend.** Als u hebt gekozen voor een aangepaste installatie, wordt het dialoogvenster ***Doelmap*** geopend.

5.6. Aangepaste installatie - Doelmap

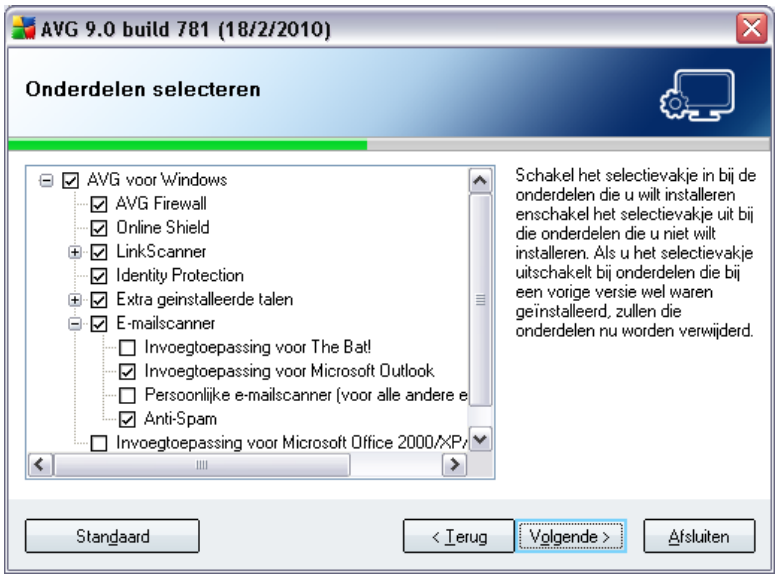


In het dialoogvenster ***Doelmap*** kunt u opgeven op welke locatie **AVG 9 Internet Security** moet worden geïnstalleerd. Standaard wordt AVG geïnstalleerd in de map Program Files op station C:. Als de map nog niet bestaat, wordt u in een nieuw dialoogvenster gevraagd te bevestigen dat AVG de map voor u moet maken.

Als u de voorkeur geeft aan een andere locatie, klikt u op de knop ***Bladeren*** om de mapstructuur weer te geven, en selecteert u de map van uw keuze.

Klik op de knop ***Volgende*** om uw keuze te bevestigen.

5.7. Aangepaste installatie - Onderdelen selecteren



Het dialoogvenster***Onderdelen selecteren*** bevat een overzicht van alle onderdelen van **AVG 9 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. Alleen die onderdelen worden voor installatie weergegeven in het dialoogvenster Onderdelen selecteren!

- ***Taalselectie***

  In de lijst met te installeren onderdelen kunt u opgeven in welke talen AVG moet worden geïnstalleerd. Schakel het selectievakje ***Extra geïnstalleerde talen*** in en selecteer daarna de gewenste talen in het menu.

- ***Invoegtoepassingen e-mailscanner***

  Klik op het item ***E-mailscanner*** om op te geven welke invoegtoepassing moet worden geïnstalleerd om de beveiliging van uw elektronische post te garanderen. Standaard wordt de ***invoegtoepassing voor Microsoft Outlook***geïnstalleerd.Als de licentie die u hebt gekocht, ook geldig is voor ***Anti-Spam***, zal dat onderdeel automatisch ook worden geïnstalleerd.U kunt ook kiezen voor de ***invoegtoepassing voor The Bat!*** Als u een andere e-mailclient gebruikt (*MS Exchange, Qualcomm Eudora, ...*), kiest u de optie ***Persoonlijke e-mailscanner*** voor automatische beveiliging van uw e-mailcommunicatie, ongeacht welk e-

mailprogramma u gebruikt.

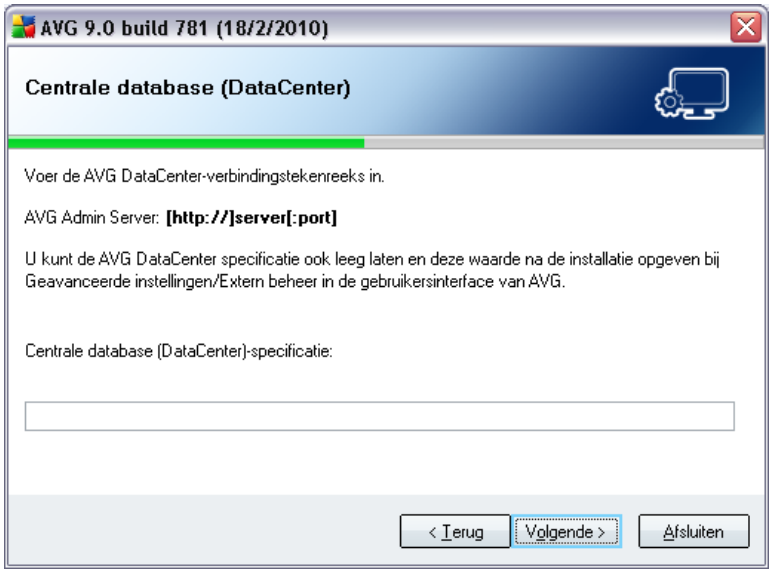
- ***Extern beheer***

  Als u van plan bent uw computer in een later stadium aan te sluiten op AVG Extern beheer, schakelt u het desbetreffende selectievakje voor installatie ook in.

Klik op de knop ***Volgende*** om verder te gaan.

5.8. AVG DataCenter

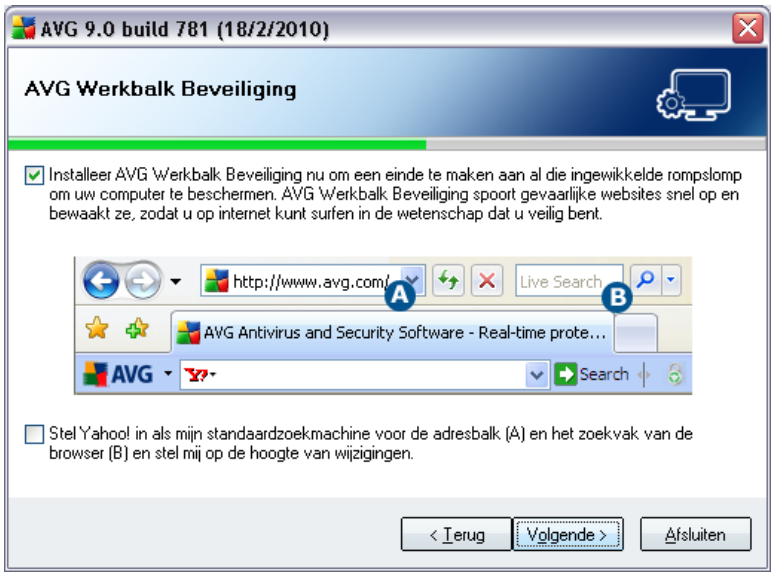
Als u een AVG-netwerklicentie gebruikt en in het vorige dialoogvenster ***Aangepaste installatie - Onderdelen selecteren*** hebt gekozen voor installatie van het item ***Extern beheer***, moet u parameters opgeven voor het ***AVG DataCenter***



Geef in het tekstveld ***AVG DataCenter specificatie*** de verbindingsstring naar ***AVG DataCenter*** op in de vorm: *server:poort*. Als die informatie op het moment niet beschikbaar is, kunt u het veld leeg laten en kunt u de instelling later opgeven in het dialoogvenster ***Geavanceerde instellingen / Extern beheer***.

Opmerking: *raadpleeg de gebruikershandleiding voor de AVG Network Edition voor meer informatie over AVG Extern beheer; u kunt die handleiding downloaden van de website van AVG (http://www.avg.com/).*

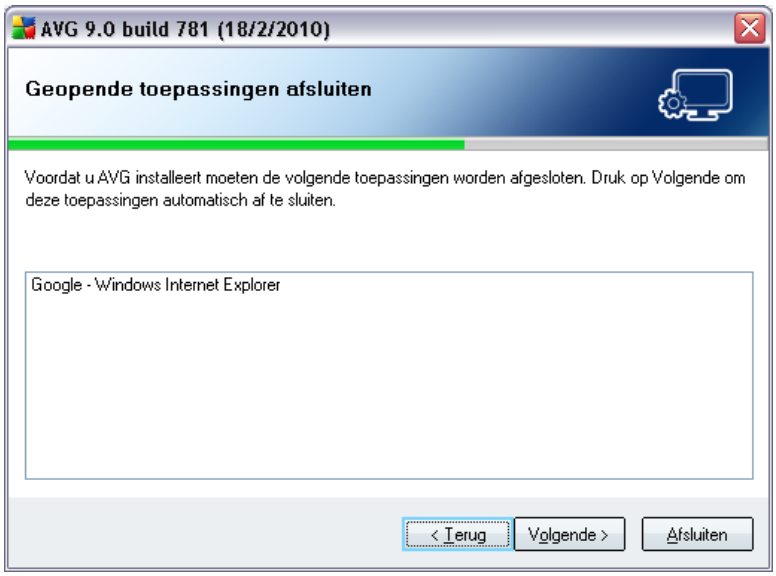
5.9. AVG Werkbalk Beveiliging



In het dialoogvenster ***AVG Werkbalk Beveiliging*** bepaalt u of u de ***AVG Werkbalk Beveiliging***wilt installeren (*controle van de zoekresultaten van de ondersteunde internetzoekmachines*). Dit onderdeel wordt automatisch in uw internetbrowser geïnstalleerd (*browsers die momenteel ondersteund worden, zijn Microsoft Internet Explorer versie 6.0 of hoger en Mozilla Firefox versie 2.0 of hoger) als u de standaardinstellingen ongewijzigd laat, en biedt een uitgebreide online bescherming terwijl u op internet surft.*

U hebt ook de mogelijkheid om Yahoo! te kiezen als uw standaard zoekmachine. Als u dit wilt, schakelt u het betreffende selectievakje in.

5.10. Geopende toepassingen afsluiten



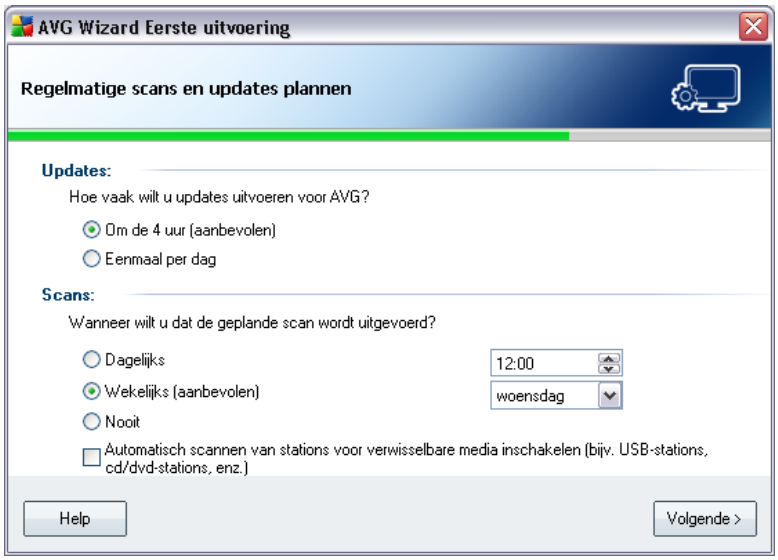
Het dialoogvenster ***Geopende toepassingen afsluiten*** wordt alleen weergegeven tijdens de installatieprocedure als er tegelijkertijd andere conflicterende programma's op uw computer worden uitgevoerd. In dat geval wordt er een lijst weergeven van de programma's die u moet sluiten om de installatieprocedure succesvol te kunnen voltooien. Klik op de knop ***Volgende*** om te bevestigen dat u deze programma's wilt sluiten en om naar de volgende stap te gaan.

5.11. AVG installeren

In het dialoogvenster ***AVG installeren*** wordt de voortgang van de installatieprocedure weergegeven, u hoeft zelf niets te doen:

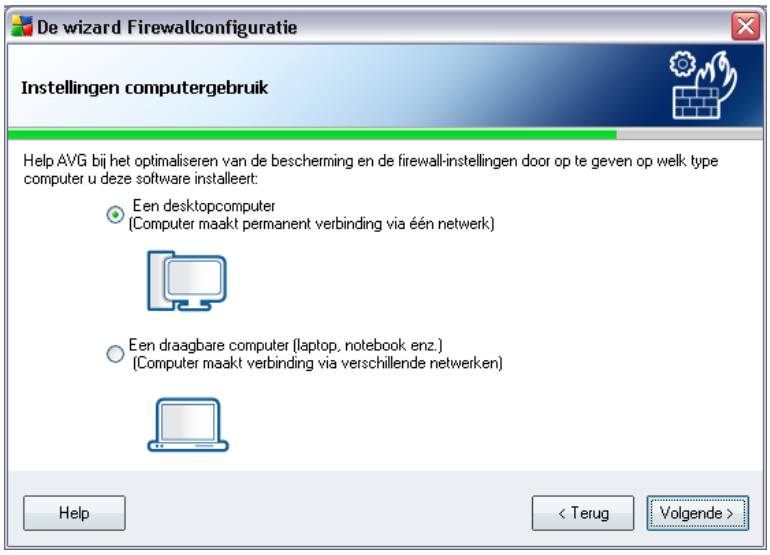
Als het installatieproces is voltooid, wordt automatisch het volgende dialoogvenster geopend.

5.12. Regelmatige scans en updates plannen



Geef in het dialoogvenster ***Regelmatige scans en updates plannen*** een interval op, waarmee moet worden gecontroleerd op de beschikbaarheid van updatebestanden, en leg vast op welk moment de geplande scan moet worden gestart. Het is raadzaam de standaardinstellingen aan te houden. Klik op de knop ***Volgende*** om door te gaan.

5.13. Instellingen computergebruik



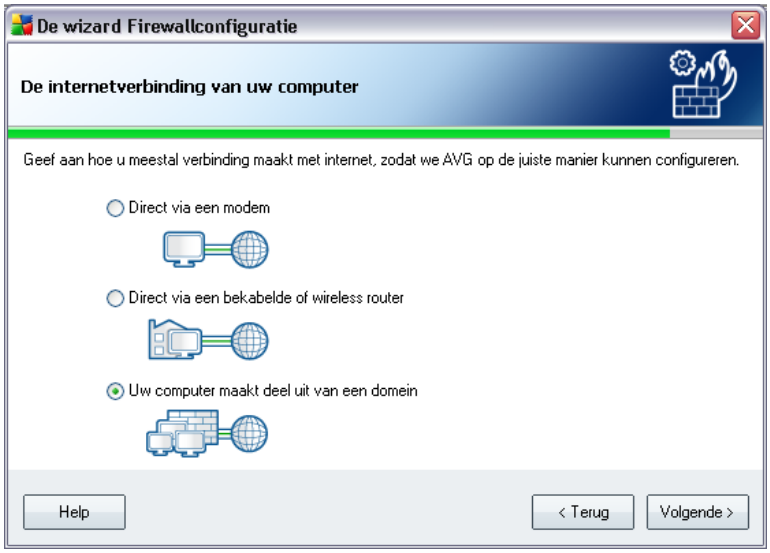
In dit dialoogvenster vraagt de ***wizard Firewallconfiguratie*** u naar het type computer dat u gebruikt. Een notebook bijvoorbeeld, die op vele locaties een internetverbinding maakt (*luchthavens, hotelkamers, enz.*), vereist strengere beveiligingsregels dan een computer in een domein (*zoals een bedrijfsnetwerk.*). Op basis van het geselecteerde type gebruik van de computer worden de standaardregels voor de ***Firewall*** aangepast voor een ander beveiligingsniveau.

U kunt kiezen uit twee opties:

- ***Desktopcomputer***
- ***Draagbare computer***

Bevestig uw selectie door op de knop ***Volgende*** te klikken, waarna het volgende dialoogvenster wordt weergegeven.

5.14. De internetverbinding van uw computer



In dit dialoogvenster vraagt de ***Wizard Firewallconfiguratie*** u hoe uw computer met internet is verbonden. Op basis van het geselecteerde verbindingstype worden de standaardregels voor de ***Firewall*** aangepast voor een ander beveiligingsniveau.

U kunt kiezen uit twee opties:

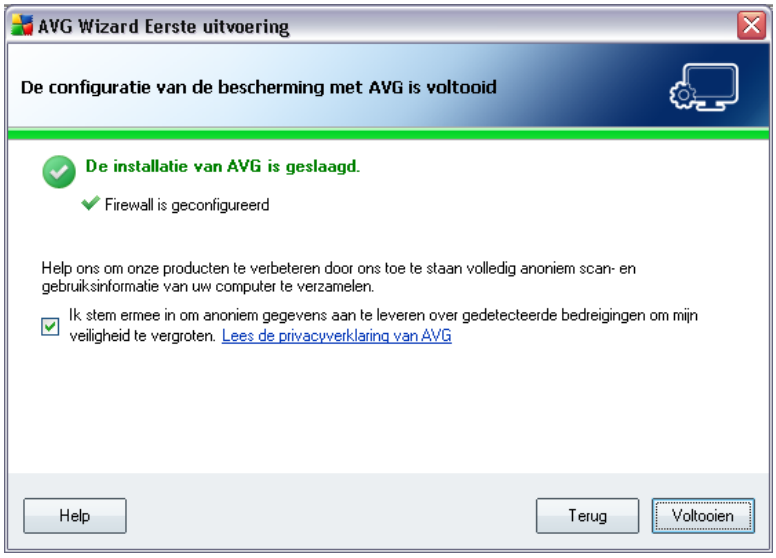
- ***Direct via een modem***

- ***Direct via een bekabelde of wireless router***
- ***Uw computer maakt deel uit van een domein***

Selecteer het verbindingstype dat de verbinding van uw computer met internet het beste beschrijft.

Bevestig uw selectie door op de knop ***Volgende*** te klikken, waarna het volgende dialoogvenster wordt weergegeven.

5.15. Configuratie AVG bescherming is voltooid



Uw **AVG 9 Internet Security** is nu geconfigureerd.

In dit dialoogvenster bepaalt u of u de optie voor het anoniem rapporteren van exploits en kwaadaardige websites aan AVG Viruslabs wilt inschakelen. Als u dat wilt, selecteert u het selectievakje ***Ik stem ermee in om ANONIEM gegevens aan te leveren over gedetecteerde bedreigingen om mijn veiligheid te vergroten***.

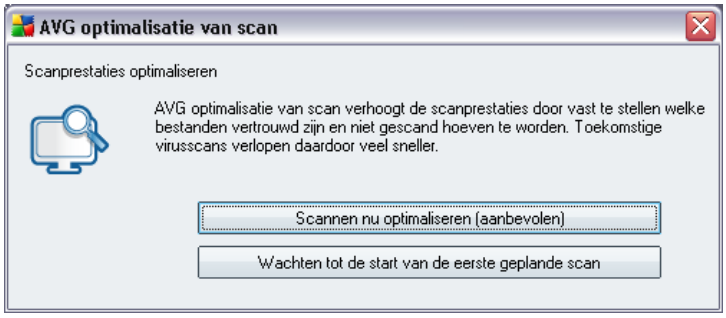
Klik daarna op de knop ***Voltooien***. Mogelijk moet u een herstart van de computer uitvoeren voordat AVG actief kan worden.

6. Na de installatie

6.1. Scanoptimalisatie

Met de functionaliteit voor optimaal scannen worden de *Windows*- en *Program Files*-mappen doorzocht, bestanden gedetecteerd (*momenteel zijn dit bestanden van het type *.exe, *.dll en *.sys*) en informatie over deze bestanden opgeslagen. De volgende keer dat deze bestanden worden gebruikt, worden ze niet opnieuw gescand. Dit vermindert de scantijd aanzienlijk.

Nadat de installatieprocedure is voltooid, wordt u in een nieuw dialoogvenster gevraagd of u het scannen wilt optimaliseren:



We raden u aan deze optie te gebruiken en het optimalisatieproces voor scannen te optimaliseren door op de knop ***Scannen nu optimaliseren*** te drukken.

6.2. Het product registreren

Registreer na het voltooien van de installatie van **AVG 9 Internet Security** uw product online op de website van AVG (http://www.avg.com/), pagina***Registratie*** (*Volg de instructies op de pagina*). Na de registratie krijgt u volledige toegang tot uw gebruikersaccount bij AVG, de AVG Update nieuwsbrief en andere services die alleen beschibaar zijn voor geregistreerde gebruikers.

6.3. Toegang tot gebruikersinterface

U kunt de ***AVG gebruikersinterface*** op meerdere manieren openen:

- Dubbelklik op het pictogram van AVG in het systeemvak
- Dubbelklik op het pictogram van AVG op het bureaublad

- Kies ***Start/Alle Programma's/AVG 9.0/AVG Gebruikersinterface***

6.4. Volledige computerscan

Het risico bestaat dat er een computervirus naar uw computer is overgebracht voordat u **AVG 9 Internet Security** hebt geïnstalleerd. Voer daarom een volledige ***scan van de computer*** uit om zeker te weten dat uw pc niet geïnfecteerd is.

Zie voor instructies voor het uitvoeren van een ***scan van uw computer*** het hoofdstuk ***AVG scannen***.

6.5. Eicar-test

Als u zeker wilt weten of **AVG 9 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. Het onderdeel ***Online shield*** geeft onmiddellijk een waarschuwing weer nadat u de download van het testbestand hebt bevestigd. Deze waarschuwing toont aan dat AVG goed op uw computer is geïnstalleerd.

U kunt ook de gecomprimeerde versie van het EICAR 'virus' downloaden van http://www.eicar.com (als eicar_com.zip). ***Online Shield*** laat toe dat u dit bestand downloadt en op uw locale schijf opslaat, maar zodra u de zip probeert uit te pakken, detecteert ***Resident Shield*** het 'virus'. **Als het Eicar-testbestand niet als virus door AVG wordt gedetecteerd, moet u uw programmaconfiguratie opnieuw controleren.**

6.6. AVG standaardconfiguratie

De standaardconfiguratie (*dat wil zeggen de manier waarop de toepassing functioneert meteen na installatie*) van **AVG 9 Internet Security** is het werk van de leverancier van de software: alle onderdelen en functies zijn zo ingesteld dat de toepassing optimaal presteert.

Wijzig de configuratie van AVG niet, tenzij er een goede reden is om dat wel te doen! Wijzigingen in de instellingen dienen alleen te worden uitgevoerd door ervaren gebruikers.

U kunt een paar minder belangrijke instellingen van AVG onderdelen meteen in de gebruikersinterface van de onderdelen wijzigen. Als u de AVG configuratie beter op uw wensen wilt laten aansluiten, opent u ***Geavanceerde instellingen AVG***: selecteer in het systeemmenu de optie ***Extra/Geavanceerde instellingen*** en bewerk de configuratie van AVG in het dialoogvenster ***Geavanceerde instellingen AVG*** dat dan wordt geopend.

7. AVG gebruikersinterface

AVG 9 Internet Security wordt geopend met het hoofdvenster:

Het hoofdvenster is onderverdeeld in een aantal secties:

- ***Systeemmenu*** *(de menubalk boven in het venster)*, het standaardmenu voor het navigeren naar alle onderdelen, services en functies van AVG - details >>
- ***Info Beveiligingsstatus*** *(bovenste deel van het venster)*, informatie over de huidige status van AVG - details >>
- ***Snelkoppelingen*** *(linker deelvenster)*, koppelingen naar de belangrijkste en meest gebruikte AVG-functies - details >>

- ***Onderdelenoverzicht*** *(centrale deel van het venster)*, overzicht van alle geïnstalleerde onderdelen van AVG - details >>

- ***Statistieken*** *(links onder in het venster)*, alle statistische gegevens over de uitvoering van de programma's - details >>

- ***Pictogram systeemvak*** *(rechts onder in het bureaublad van Windows, in het systeemvak)*, indicatie van de huidige status van AVG - details >>

7.1. Systeemmenu

Het ***Systeemmenu*** is de standaard navigatiestructuur die in alle Windows-toepassingen wordt gebruikt. Deze is horizontaal aan de bovenrand van het hoofdvenster van **AVG 9 Internet Security** geplaatst. Met behulp van het systeemmenu heeft u toegang tot de AVG onderdelen, functies en services.

Het systeemmenu is onderverdeeld in vijf secties:

7.1.1. Bestand

- ***Afsluiten*** - afsluiten van de **AVG 9 Internet Security**-gebruikersinterface. De AVG toepassing zal echter op de achtergrond actief blijven en uw computer is nog steeds beschermd!

7.1.2. Onderdelen

Het systeemmenu-item ***Onderdelen*** heeft koppelingen naar alle geïnstalleerde AVG-onderdelen:

- ***Systeemoverzicht*** - Weergeven van het standaard dialoogvenster met het overzicht van alle geïnstalleerde onderdelen en hun status

- ***Anti-Virus*** - openen van de standaardpagina van het onderdeel ***Anti-Virus***

- ***Anti-Rootkit*** - openen van de standaardpagina van het onderdeel ***Anti-Rootkit***

- ***Anti-Spyware*** - openen van de standaardpagina van het onderdeel ***Anti-Spyware***

- ***Firewall*** - openen van de standaardpagina van het onderdeel ***Firewall***

- ***LinkScanner*** - openen van de standaardpagina van het onderdeel ***LinkScanner***

- ***Systeemprogramma*** - openen van de standaardpagina van het onderdeel

Systeemprogramma

- ***Anti-Spam*** - openen van de standaardpagina van het onderdeel ***Anti-Spam***
- ***E-mailscanner*** - openen van de standaardpagina van het onderdeel ***E-mailscanner***
- ***ID Protection*** / openen van de standaardpagina van het onderdeel ***Identity Protection***
- ***Licentie*** - openen van de standaardpagina van het onderdeel ***Licentie***
- ***Online Shield*** - openen van de standaardpagina van het onderdeel ***Online Shield***
- ***Resident Shield*** - openen van de standaardpagina van het onderdeel ***Resident Shield***
- ***Updatebeheer*** - openen van de standaardpagina van het onderdeel ***Updatebeheer***

7.1.3. Historie

- ***Scanresultaten*** - de AVG testinterface wordt geopend, in het bijzonder het dialoogvenster ***Overzicht scanresultaten***
- ***Resident Shield detectie*** - er wordt een overzicht geopend met bedreigingen die zijn gedetecteerd door ***Resident Shield***
- ***E-mailscannerdetectie*** - er wordt een overzicht geopend met bijlagen bij e-mailberichten die als gevaarlijk zijn gedetecteerd door het onderdeel ***E-mailscanner***
- ***Online Shield resultaten*** - er wordt een overzicht geopend met bedreigingen die zijn gedetecteerd door ***Online Shield***
- ***Quarantaine*** - de interface van de ***Quarantaine*** wordt geopend, waar AVG alle gedetecteerde infecties opslaat die om de een of andere reden niet automatisch kunnen worden hersteld. In de quarantaine worden de geïnfecteerde bestanden geïsoleerd, zodat uw computer veilig blijft, terwijl het opslaan van de bestanden eventueel herstel van de bestanden in de toekomst mogelijk maakt.
- ***Gebeurtenishistorie Logboek*** - het dialoogvenster wordt geopend met de geschiedenis van alle vastgelegde acties van **AVG 9 Internet Security** .

- ***Firewall*** - het dialoogvenster Firewall-instellingen wordt geopend, en op het tabblad ***Logboeken*** staat een gedetailleerd overzicht van alle acties die Firewall heeft ondernomen

7.1.4. Hulpmiddelen

- ***Computer scannen*** - de AVG Scaninterface wordt geopend en een scan van de volledige computer wordt gestart

- ***Scan geselecteerde map*** - de AVG Scaninterface wordt geopend, zodat u in de bestandsstructuur van uw computer mappen en bestanden kunt selecteren die moeten worden gescand

- ***Bestand scannen*** - u kunt in de bestandsstructuur van de computer een enkel bestand selecteren dat u wilt scannen

- ***Update*** - automatisch de updateprocedure starten van **AVG 9 Internet Security**

- ***Bijwerken vanuit directory*** - de updateprocedure wordt gestart aan de hand van updatebestanden in een bepaalde 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.

- ***Geavanceerde instellingen*** - het dialoogvenster ***Geavanceerde instellingen AVG*** wordt geopend waarin u de configuratie van **AVG 9 Internet Security** kunt wijzigen. Over het algemeen is het raadzaam de standaardinstellingen aan te houden, zoals die zijn ingesteld door de leverancier van de software.

- ***Firewall-instellingen*** - er wordt een standalone dialoogvenster geopend voor geavanceerde configuratie van het onderdeel ***Firewall***

7.1.5. Help

- ***Inhoud*** – de Help-bestanden van AVG worden geopend

- ***Online Help*** - de website van AVG (http://www.avg.com/) wordt geopend op de pagina voor klantenservice

- ***Uw AVG-web*** - de website van AVG (http://www.avg.com/) openen

- ***Over virussen & bedreigingen*** – de online ***Virusencyclopedie***wordt geopend, waarin u gedetailleerde informatie kunt zoeken over bekende virussen

- ***Opnieuw activeren*** - het dialoogvenster ***AVG activeren*** wordt geopend met de gegevens die u heeft opgegeven in het dialoogvenster ***AVG aanpassen*** van de installatieprocedure. In dit dialoogvenster kunt u uw licentienummer invoeren ter vervanging van ofwel het verkoopnummer (*het nummer waarmee u AVG heeft geïnstalleerd*), ofwel het oude licentienummer (*bijvoorbeeld bij het upgraden naar een nieuw product van AVG*).

- ***Nu registreren*** - verbinding maken met de registratiepagina van de website van AVG (http://www.avg.com/). Voer uw registratiegegevens in; alleen klanten die hun AVG product registreren komen in aanmerking voor gratis technische ondersteuning.

Opmerking*: Als u de proefversie van* **AVG 9 Internet Security** *gebruikt, worden de laatste twee items weergegeven als* ***Nu kopen*** *en* ***Activeren****, zodat u de volledige versie van het programma meteen kunt kopen. Als u* **AVG 9 Internet Security** *hebt geïnstalleerd met een verkoopnummer, worden deze items weergegeven als* ***Registreren*** *en* ***Activeren****. Zie voor meer informatie het gedeelte Licentie in deze documentatie.*

- ***Info over AVG*** - het dialoogvenster ***Info*** wordt geopend met vijf tabbladen met gegevens over de programmanaam, versie van programma en virusdatabase, systeeminformatie, licentieverklaring en contactgegevens van ***AVG Technologies CZ***.

7.2. Info Beveiligingsstatus

De sectie ***Info Beveiligingsstatus*** bevindt zich in het bovenste deel van het hoofdvenster van AVG. In deze sectie staat altijd informatie over de huidige beveiligingsstatus van **AVG 9 Internet Security**. Hieronder volgt een overzicht van de pictogrammen die in deze sectie kunnen worden weergegeven, en hun betekenis:

 Het groene pictogram duidt erop dat AVG volledig functioneert. Uw computer is volledig beveiligd, de bestanden zijn bijgewerkt en alle geïnstalleerde onderdelen werken correct.

 Het oranje pictogram is een waarschuwing dat een of meer onderdelen onjuist zijn geconfigureerd en dat u de desbetreffende eigenschappen/ instellingen moet controleren. Er is geen wezenlijk probleem opgetreden in AVG;

waarschijnlijk hebt u gewoon om de een of andere reden een onderdeel uitgeschakeld. U wordt nog steeds beschermd door AVG. Neem echter wel even de tijd om de instellingen van het problematische onderdeel te controleren! De naam van het onderdeel wordt aangegeven in de sectie ***Info Beveiligingsstatus*** ..

Dit pictogram wordt ook weergegeven als u om één of andere reden hebt besloten om de foutstatus van een onderdeel te negeren (*de optie "Onderdeelstatus negeren" is beschikbaar via het contextmenu dat wordt geopend door te klikken met de rechtermuisknop op het pictogram van het betreffende onderdeel in het onderdeeloverzicht van het hoofdvenster van AVG*). U dient deze optie mogelijk te gebruiken in een specifieke situatie, maar het wordt ten zeerste aanbevolen om de optie "***Onderdeelstatus negeren***" zo snel mogelijk uit te schakelen.

 Een rood pictogram geeft aan dat er een kritieke situatie is! Één of meer onderdelen functioneren niet correct en AVG kan 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, neem dan contact op met het team van de Technische ondersteuning van AVG.

We raden u nadrukkelijk aan de sectie Info Beveiligingsstatus goed in de gaten te houden en in het geval van een probleem, daar meteen aandacht aan te besteden en te proberen het probleem op te lossen. Uw computer loopt anders gevaar!

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

7.3. Snelkoppelingen

Met behulp van snelkoppelingen *(in het linker deelvenster van de AVG gebruikersinterface)* kunt u snel de belangrijkste en meest gebruikte functies van AVG oproepen:

- ***Overzicht*** - klik op deze snelkoppeling om vanuit een geopend dialoogvenster van AVG terug te keren naar het Overzicht van alle geïnstalleerde onderdelen - zie het hoofdstuk ***Overzicht van onderdelen*** >>
- ***Computerscanner*** - klik op deze snelkoppeling om de scaninterface van AVG op te roepen, waarin u direct scans kunt uitvoeren, plannen en schema-instellingen kunt wijzigen - zie het hoofdstuk ***AVG scannen*** >>
- ***Nu bijwerken*** - klik op deze snelkoppeling om de interface voor updates te openen en meteen een updateprocedure voor AVG te starten - zie het hoofdstuk ***AVG updates*** >>

Deze snelkoppelingen zijn te allen tijde beschikbaar in de gebruikersinterface. Zodra u op een snelkoppeling klikt om een bepaalde procedure uit te voeren, wordt weliswaar een nieuw dialoogvenster geopend, maar de snelkoppelingen blijven niettemin beschikbaar. Bovendien wordt de uitgevoerde procedure grafisch weergegeven.

7.4. Overzicht van onderdelen

De sectie ***Overzicht van onderdelen*** staat in het middelste gedeelte van de AVG gebruikersinterface. De sectie is onderverdeeld in twee gedeelten:

- Een overzicht van alle geïnstalleerde onderdelen dat bestaat uit een deelvenster met het pictogram van het onderdeel en de informatie of het desbetreffende onderdeel actief is of niet.
- Beschrijving van een geselecteerd onderdeel

De sectie ***Overzicht van onderdelen*** in **AVG 9 Internet Security**, bevat informatie over de volgende onderdelen:

- ***Anti-Virus*** biedt uw computer bescherming tegen virussen die uw computer proberen binnen te dringen - details >>

- ***Anti-Spyware*** scant toepassingen op de achtergrond terwijl u die uitvoert - details >>
- ***Anti-Spam*** controleert alle binnenkomende e-mailberichten en markeert ongewenste e-mails als SPAM - details >>
- ***Firewall*** beheert hoe uw computer gegevens uitwisselt met andere computers op internet of in het lokale netwerk - details >>
- ***LinkScanner*** controleert zoekresultaten die in uw browser worden weergegeven - details >>
- ***Anti-Rootkit*** detecteert programma's en technologieën die proberen malware te camoufleren - details >>
- ***Systeemprogramma's*** bieden een gedetailleerd overzicht van de AVG-omgeving en informatie over het besturingssysteem - details >>
- ***E-mailscanner*** controleert alle binnenkomende en uitgaande e-mail op virussen - details >>
- ***ID Protection*** - anti-malware-onderdeel gericht op het voorkomen van diefstal van waardevolle persoonlijke digitale gegevens - details >>
- ***Licentie*** bevat informatie over het licentienummer, -type en de vervaldatum - details >>
- ***Online Shield*** scant alle gegevens die door een webbrowser worden gedownload - details >>
- ***Resident Shield*** wordt op de achtergrond uitgevoerd en scant bestanden als ze worden gekopieerd, geopend of opgeslagen - details >>
- ***Updatebeheer*** beheert alle AVG updates - details >>

Klik op het pictogram van een onderdeel om het in het overzicht van onderdelen te selecteren. Dan wordt in het onderste deel van de gebruikersinterface ook de beschrijving van de basisfunctionaliteit van het onderdeel weergegeven. Dubbelklik op een pictogram om de interface van het onderdeel, met een lijst elementaire statistische gegevens, te openen.

Klik met de rechtermuisknop op een pictogram van een onderdeel om een contextmenu uit te vouwen: behalve het openen van de grafische interface van het onderdeel kunt u ook ***Onderdeelstatus negeren*** selecteren. Selecteer deze optie om aan te geven dat u zich bewust bent van de foutstatus van het onderdeel, maar dat u om een

bepaalde reden uw AVG ongewijzigd wilt laten en niet wilt worden gewaarschuwd door het systeemvakpictogram.

7.5. Statistieken

De sectie***Statistieken*** bevindt zich links onder in de AVG gebruikersinterface. Deze bevat een lijst met informatie over het functioneren van het programma.

- ***Laatste scan*** - de datum waarop de laatst scan is uitgevoerd
- ***Last update*** - de datum waarop de laatste update is uitgevoerd
- ***Virus DB*** - informatie over de huidige geïnstalleerde versie van de virusdatabase
- ***AVG-versie*** - informatie over de geïnstalleerde AVG-versie *(een nummer met de opmaak 9.0.xx, waarbij 9.0 de productversie is en xx voor het typenummer staat)*
- ***Vervaldatum licentie*** - de vervaldatum van uw AVG-licentie

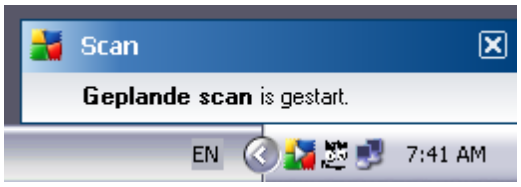
7.6. Systeemvakpictogram

Het systeemvakpictogram (*op de taakbalk van Windows*) geeft de huidige status van **AVG 9 Internet Security** aan. Het pictogram wordt steeds weergegeven in het systeemvak, ongeacht of het hoofdvenster van AVG is geopend of gesloten.

Als alle kleuren te zien zijn  , geeft het ***systeemvakpictogram*** aan dat alle AVG-onderdelen actief zijn en geheel naar behoren werken. Het systeemvakpictogram van AVG kan ook worden weergegeven in vier kleuren als AVG een foutstatus heeft, maar u geheel op de hoogte bent van deze situatie en bewust hebt besloten ***de onderdeelstatus te negeren***.

Een pictogram met een uitroepteken  duidt op een probleem (*niet-actief onderdeel, foutstatus, enz.*). Dubbelklik op het ***systeemvakpictogram*** om het hoofdvenster te openen en een onderdeel aan te passen.

Het systeemvakpictogram geeft bovendien informatie over huidige activiteiten van AVG en mogelijke statuswijzigingen in het programma (*bijv. automatische start van een geplande scan of update, Firewall profielschakeling, een wijziging van een onderdeelstatus, een foutstatus, ...*) via een pop-upvenster dat wordt geopend vanuit het systeemvakpictogram van AVG:



U kunt door op het ***systeemvakpictogram*** te dubbelklikken op elk gewenst moment snel het hoofdvenster van AVG openen. Als u met de rechtermuisknop op het ***systeemvakpictogram*** klikt, opent u een snelmenu met de volgende opties:

- ***AVG gebruikersinterface openen*** – klik op de optie als u de AVG gebruikersinterface wilt openen
- ***Update*** – onmiddellijk starten van een update

8. AVG onderdelen

8.1. Anti-Virus

8.1.1. Anti-Virus Principes

De scan-engine van de antivirussoftware scant alle bestanden en alle activiteiten waarbij bestanden betrokken zijn (openen/sluiten van bestanden, enz.) op bekende virussen. Elk gedetecteerd virus wordt geblokkeerd, zodat het geen activiteit kan ontwikkelen, en wordt daarna schoongemaakt of in quarantaine geplaatst. De meeste antivirusprogramma's gebruiken ook heuristische analyse, waar bij bestanden worden gescand op typische kenmerken van virussen, zogenaamde virale handtekeningen. Dat betekent dat de virusscanner een nieuw, nog onbekend virus kan detecteren, als dat virus bepaalde typerende kenmerken heeft van bestaande virussen.

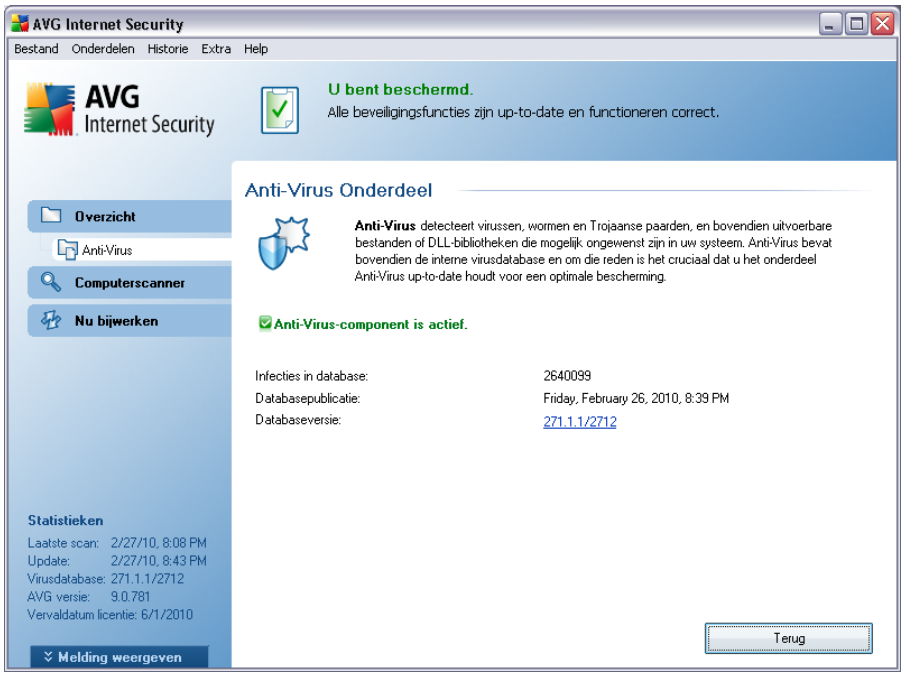
De belangrijste functie van bescherming tegen virussen is het verhinderen van activiteit van bekende virussen!

Omdat bij het gebruik van slechts één technologie een bepaald virus misschien over het hoofd kan worden gezien of niet wordt herkend, zijn in ***Anti-Virus*** diverse technologieën gecombineerd om te garanderen dat uw computer wordt beschermd:

- Scannen - hiermee wordt naar tekenreeksen gezocht die kenmerkend voor een bepaald virus zijn
- Heuristische analyse - dynamische emulatie van de instructies van gescande objecten in een virtuele computeromgeving
- Algemene detectie - detectie van instructies die kenmerkend zijn voor een bepaald virus of een bepaalde groep virussen

AVG kan bovendien uitvoerbare toepassingen en DLL-bibliotheken analyseren en detecteren die mogelijk ongewenst zijn binnen het systeem. Dergelijke bedreigingen noemen we potentieel ongewenste programma's (verschillende typen spyware, adware, enz.). Daarnaast scant AVG uw systeemregister op verdachte sleutels, tijdelijke internetbestanden en zogeheten tracking-cookies. U kunt hierbij instellen dat alle mogelijk schadelijke items op dezelfde wijze moeten worden afgehandeld als andere infecties.

8.1.2. Anti-virus interface



De interface van het onderdeel ***Anti-Virus*** biedt elementaire informatie over de functionaliteit van het onderdeel, de huidige status (*Anti-Virus-component is actief.*), en een beknopt overzicht met ***Anti-Virus***-statistieken:

- ***Infectiedefinities*** - het aantal in de meest actuele versie van de virusdatabase gedefinieerde virussen
- ***Laatste update database*** - de datum en het tijdstip waarop de virusdatabase voor het laatst is bijgewerkt
- ***Databaseversie*** - het nummer van de laatste databaseversie; dit nummer wordt bij iedere nieuwe versie één hoger

Het dialoogvenster van dit onderdeel heeft maar één knop (***Terug***) - klik op deze knop om terug te keren naar de standaard AVG gebruikersinterface (Overzicht van onderdelen).

Opmerking: *De leverancier heeft alle onderdelen van AVG zo ingesteld dat ze optimaal presteren. Wijzig de configuratie van AVG niet, tenzij er een goede reden is om dat wel te doen. Wijzigingen in de instellingen dienen alleen te worden uitgevoerd door ervaren gebruikers. Als u de AVG-configuratie dient te wijzigen, selecteert u in*

*het systeemmenu de optie**Tools / Geavanceerde instellingen** en bewerkt u de AVG-configuratie in het nieuw geopende dialoogvenster AVG Geavanceerde instellingen.*

8.2. Anti-Spyware

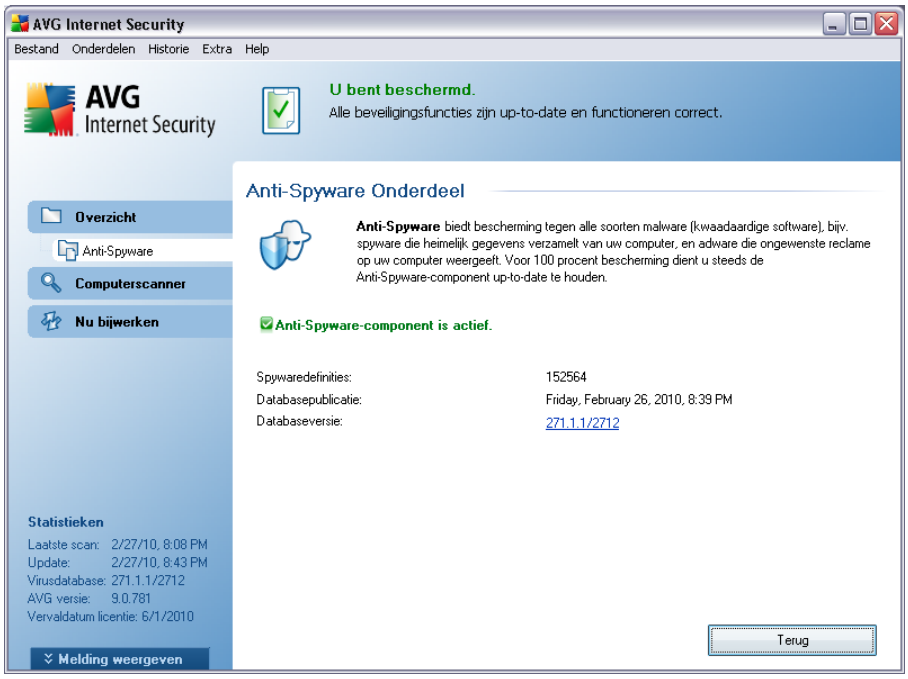
8.2.1. Anti-Spyware Principes

Spyware wordt meestal gedefinieerd als een soort malware: software die informatie op een computer verzamelt zonder medeweten of toestemming van de gebruiker. Sommige spywaretoepassingen worden opzettelijk geïnstalleerd en bevatten vaak reclame, pop-ups of andere soorten ongewenste software.

Spyware en malware worden voornamelijk verspreid via websites met een inhoud die mogelijk gevaarlijk is. Daarnaast wordt dergelijke software ook verspreid via e-mailberichten en via wormen en virussen. De meest geschikte beveiligingsmethode is een achtergrondscanner die altijd is ingeschakeld, zoals ***Anti-Spyware***. Dit onderdeel werkt als een resident shield en scant uw toepassingen op de achtergrond wanneer deze worden uitgevoerd.

Het is echter mogelijk dat uw computer reeds malware bevatte op het moment dat u AVG op de computer hebt geïnstalleerd, of dat u **AVG 9 Internet Security** niet regelmatig hebt bijgewerkt met de recentste database- en programma-updates. AVG is daarom voorzien van een scanfunctie waarmee u uw computer op malware/spyware kunt scannen. Die detecteert ook slapende en niet-actieve malware, dat wil zeggen malware die al wel is gedownload, maar nog niet is geactiveerd.

8.2.2. Anti-Spyware interface



De interface van het onderdeel ***Anti-Spyware*** biedt een beknopt overzicht van de functionaliteit van het onderdeel, de huidige status (*Anti-Spyware-component is actief.*) en een paar ***Anti-Spyware***-statistieken:

- ***Spywaredefinities*** - het totale aantal spywaremonsters dat in de nieuwste versie van de spywaredatabase is gedefinieerd
- ***Laatste update database*** - de datum en het tijdstip waarop de virusdatabase voor het laatst is bijgewerkt
- ***Databaseversie*** - het nummer van de laatste spywaredatabaseversie; dit nummer wordt bij iedere nieuwe versie één hoger

Het dialoogvenster van dit onderdeel heeft maar één knop (***Terug***) - klik op deze knop om terug te keren naar de standaard AVG gebruikersinterface (Overzicht van onderdelen).

Opmerking: De leverancier van *heeft alle onderdelen van AVG zo ingesteld dat ze optimaal presteren. Wijzig de configuratie van AVG niet, tenzij er een goede reden is om dat wel te doen. Wijzigingen in de instellingen dienen alleen te worden uitgevoerd door ervaren gebruikers. Als u de AVG-configuratie dient te wijzigen, selecteert u in*

*het systeemmenu de optie**Tools / Geavanceerde instellingen** en bewerkt u de AVG-configuratie in het nieuw geopende dialoogvenster AVG Geavanceerde instellingen.*

8.3. Anti-Spam

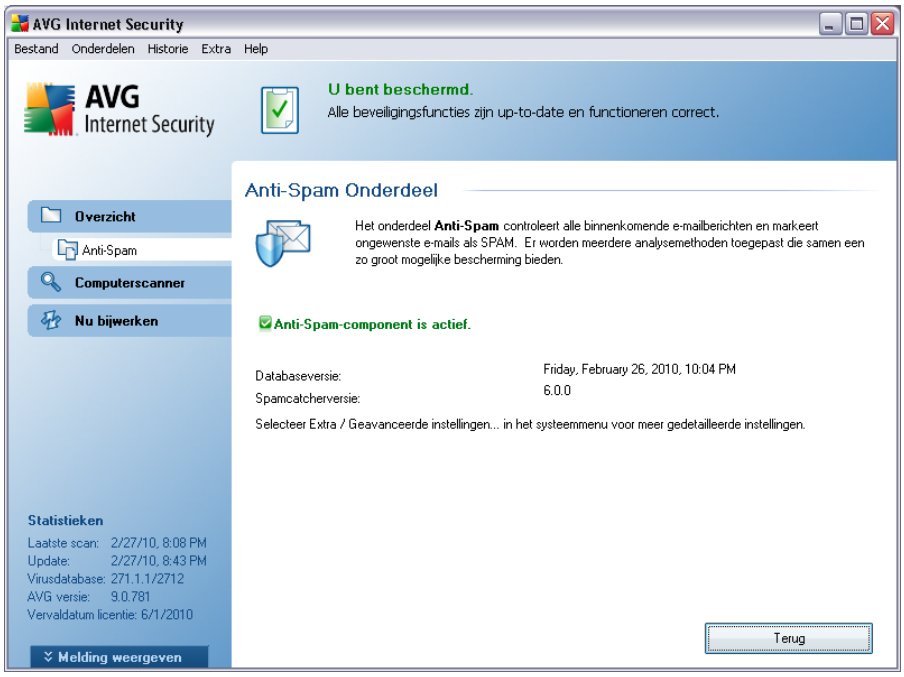
Spam verwijst naar ongewenste e-mailberichten, die meestal reclame maken voor een product of service en naar grote aantallen e-mailadressen die tegelijk verstuurd worden, waardoor de postbussen van ontvangers vol raken. Spam verwijst niet naar wettige commerciële e-mail waarvoor klanten hun toestemming hebben gegeven. Spam is niet alleen vervelend, maar kan ook een bron zijn van zwendel, virussen of aanstootgevende inhoud.

8.3.1. Anti-Spam principes

AVG Anti-Spam controleert alle binnenkomende e-mailberichten en markeert ongewenste e-mails als spam.***AVG 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.

AVG Anti-Spam maakt gebruik van verschillende analysemethoden om elk e-mailbericht te verwerken. Dit biedt de best mogelijke bescherming tegen ongewenste e-mailberichten. ***AVG Anti-Spam*** maakt voor spamdetectie gebruik van een database die regelmatig wordt bijgewerkt. U kunt ook RBL-serversopgeven (*algemeen toegankelijke databases met e-mailadressen van bekende 'spammers'*) en handmatig e-mailadressen toevoegen aan uw Witte lijst (*nooit als spam markeren*) en Zwarte lijst (*altijd als spam markeren*).

8.3.2. Anti-Spam interface



In het dialoogvenster van het onderdeel ***Anti-Spam*** staat een korte tekst met een beschrijving van de functionaliteit van het onderdeel, informatie over de huidige status (*Anti-Spam-component is actief.*) en de volgende statistieken:

- ***Databaseversie*** - de datum en het tijdstip waarop de spamdatabase is bijgewerkt en gepubliceerd.
- ***Spamcatcherversie*** - het nummer van de nieuwste versie van de anti-spam-engine.

Het dialoogvenster van dit onderdeel heeft maar één knop (***Terug*** - klik op deze knop om terug te keren naar de standaard AVG gebruikersinterface *(Overzicht van onderdelen*).

Opmerking: *De leverancier heeft alle onderdelen van AVG zo ingesteld dat ze optimaal presteren. Wijzig de configuratie van AVG niet, tenzij er een goede reden is om dat wel te doen. Wijzigingen in de instellingen dienen alleen te worden uitgevoerd door ervaren gebruikers. Als u de AVG-configuratie dient te wijzigen, selecteert u in het systeemmenu de optie****Tools / Geavanceerde instellingen*** *en bewerkt u de AVG-configuratie in het nieuw geopende dialoogvenster AVG Geavanceerde instellingen.*

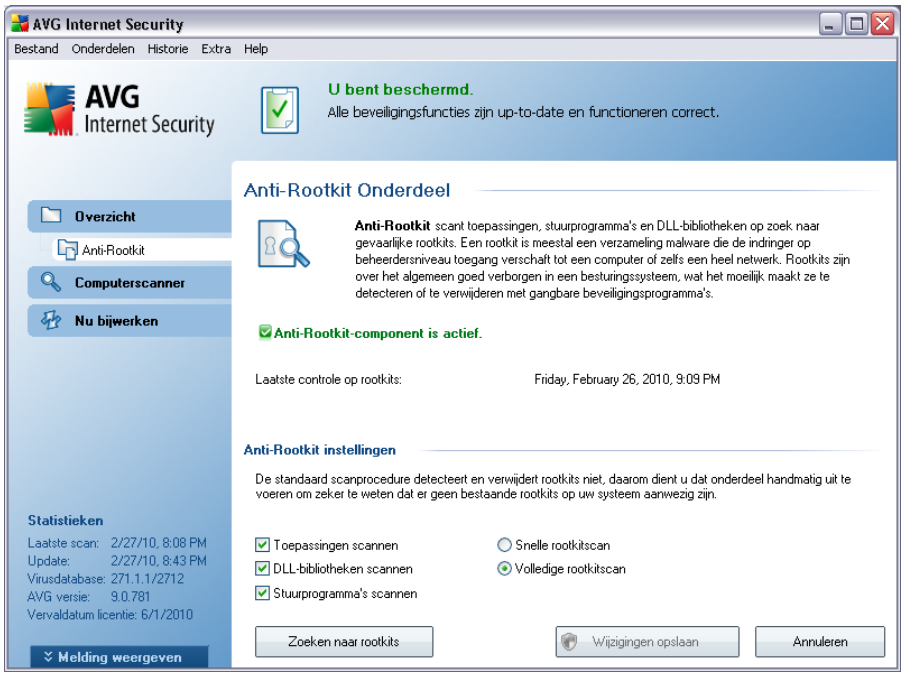
8.4. Anti-Rootkit

Een rootkit is een programma dat is ontwikkeld om de controle over een computersysteem over te nemen zonder toestemming van de eigenaren en rechtmatige beheerders van het systeem. Toegang tot de hardware is zelden vereist omdat een rootkit is bedoeld om de controle over het besturingssysteem dat op de hardware draait, over te nemen. Gewoonlijk proberen rootkits hun aanwezigheid te verbergen door het ondermijnen of ontwijken van de standaard beveiligingsmechanismen van het besturingssysteem. Vaak zijn het bovendien Trojaanse paarden die gebruikers in de waan laten dat ze veilig met hun systeem kunnen werken. De technieken die worden gebruikt om dit te bereiken omvatten bijvoorbeeld het voor bewakingsprogramma's verbergen van processen die worden uitgevoerd, of het verbergen van bestanden of systeemgegevens voor het besturingssysteem.

8.4.1. Anti-Rootkit principes

Anti-Rootkit is een speciaal ontwikkeld hulpmiddel voor het detecteren en effectief verwijderen van gevaarlijke rootkits, programma's en technologie die de aanwezigheid van schadelijke software op een computer kunnen camoufleren. ***AVG Anti-Rootkit*** kan rootkits herkennen aan de hand van een vooraf gedefinieerde set regels. We wijzen erop dat alle rootkits worden gedetecteerd (*niet alleen geïnfecteerde*). Als ***AVG Anti-Rootkit*** een rootkit detecteert, betekent dat niet automatisch dat die rootkit ook geïnfecteerd is. Soms worden rootkits gebruikt als stuurprogramma's of vormen ze een onderdeel van een onverdacht programma.

8.4.2. Anti-Rootkit interface



De gebruikersinterface van ***Anti-Rootkit*** biedt een korte beschrijving van de functionaliteit van het onderdeel, informatie over de huidige status van het onderdeel (*Anti-Rootkit-component is actief.*) en biedt bovendien informatie over de laatste keer dat de ***Anti-Rootkit***-test is uitgevoerd.

In het onderste deel van het dialoogvenster staan de ***Anti-Rootkit instellingen*** waar u een aantal elementaire parameters kunt instellen voor het scannen op de aanwezigheid van rootkits. Schakel eerst de selectievakjes in van de objecten die moeten worden gescand:

- ***Toepassingen scannen***
- ***DLL-bibliotheken scannen***
- ***Stuurprogramma's scannen***

Vervolgens kunt u de scanmodus kiezen:

- ***Snelle rootkitscan*** - scant 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*)

Beschikbare knoppen

- ***Zoeken naar rootkits*** - aangezien de rootkitscan geen geïntegreerd onderdeel is van ***Volledige computer scannen***, kunt u rechtstreeks vanuit de ***Anti-rootkit***-interface rootkitscans uitvoeren als u op deze knop klikt.

- ***Wijzigingen opslaan*** - klik op deze knop om alle wijzigingen die u in dit venster hebt uitgevoerd op te slaan en terug te keren naar de standaard***AVG-gebruikersinterface*** (Overzicht van onderdelen)

- ***Annuleren*** - druk op deze knop om terug te keren naar de standaard ***AVG-gebruikersinterface*** (Overzicht van onderdelen) zonder wijzigingen op te slaan

8.5. Systeemprogramma's

Systeemprogramma's verwijst naar een gedetailleerd overzicht van de omgeving van **AVG 9 Internet Security** en het besturingssysteem. In dit onderdeel vindt u een overzicht van:

- Processen - een lijst met processen (bijv. toepassingen die worden uitgevoerd) die op het moment van raadplegen actief zijn op de computer

- Netwerkverbindingen - lijst met op het moment van raadplegen actieve verbindingen

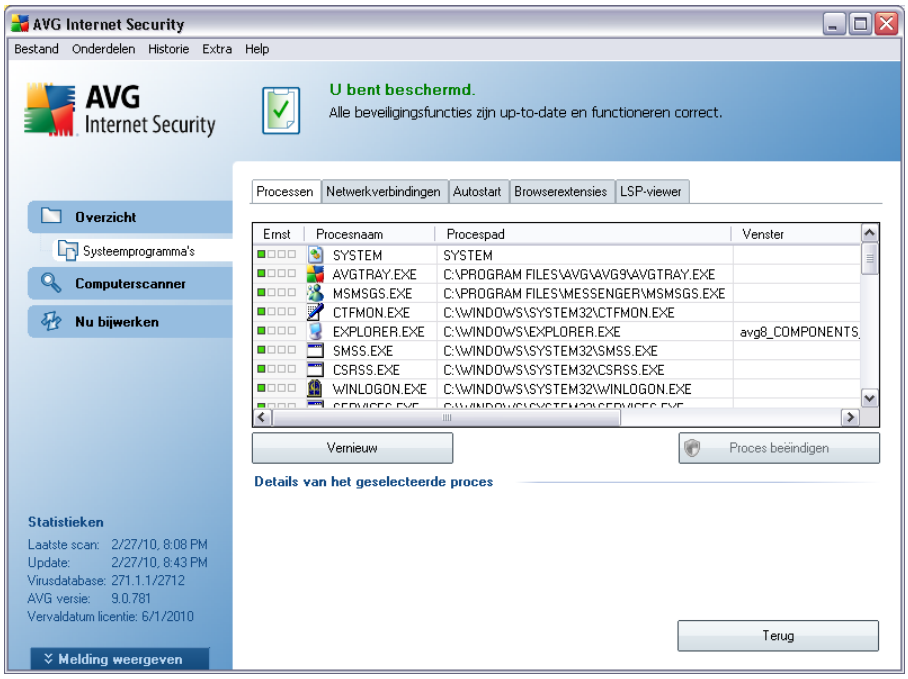
- Autostart - een lijst met alle toepassingen die worden uitgevoerd tijdens het opstarten van het Windows-systeem

- Browserextensies - een lijst met invoegtoepassingen (bijvoorbeeld toepassingen) die zijn geïnstalleerd in uw internetbrowser.

- LSP-viewer - een lijst met Layered Service Providers (LSP's)

Bepaalde overzichten kunnen worden bewerkt, maar dat wordt alleen aanbevolen aan zeer ervaren gebruikers!

8.5.1. Processen



In het dialoogvenster ***Processen*** staat een lijst met processen (*bijv. toepassingen*) die worden uitgevoerd op de computer. De lijst bestaat uit een aantal kolommen.

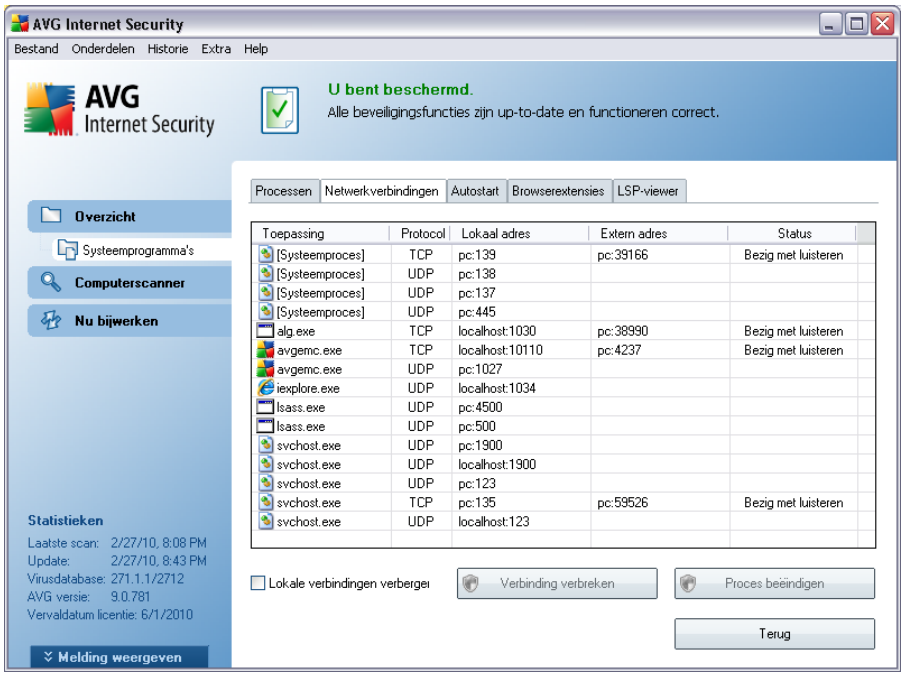
- ***Bedreigingsniveau*** - grafische aanduiding voor het bedreigingsniveau van het proces op een schaal met vier niveaus van vrij onbelangrijk (■□□□) tot kritiek (■■■■)
- ***Procesnaam*** - de naam van het proces dat momenteel wordt uitgevoerd
- ***Pad*** - het fysieke pad naar het proces dat wordt uitgevoerd
- ***Venster*** - indien van toepassing, de naam van het toepassingsvenster
- ***Internet*** - geeft aan of het uitgevoerde proces ook is verbonden met het internet (*ja/nee*)
- ***Service*** - geeft aan of het uitgevoerde proces een service betreft (*ja/nee*)
- ***PID*** - het PID (process identification number) is een uniek intern nummer waarmee Windows het proces aanduidt

Knoppen

De interface van ***Systeemprogramma's*** heeft de volgende knoppen:

- ***Vernieuwen*** - de lijst met processen bijwerken aan de hand van de huidige status
- ***Proces beëindigen*** - u kunt één of meer toepassingen selecteren en die beëindigen door op deze knop te klikken. ***Het beëindigen van toepassingen raden we u ten zeerste af, tenzij u absoluut zeker weet dat deze toepassingen een bedreiging vormen!***
- ***Terug*** - als u op deze knop klikt, keert u terug naar de standaard ***AVG-gebruikersinterface*** (Overzicht van onderdelen).

8.5.2. Netwerkverbindingen



In het dialoogvenster ***Netwerkverbindingen*** staat een lijst met verbindingen die actief zijn. De lijst is verdeeld over een aantal kolommen.

- ***Toepassing*** - naam van de toepassing met betrekking tot de verbinding (*met uitzondering van Windows 2000 waarin deze informatie niet beschikbaar is*)

- ***Protocol*** - transmissieprotocoltype dat voor de verbinding wordt gebruikt:
    - TCP - het protocol dat samen met het Internet Protocol (IP) wordt gebruikt om informatie over het internet te verzenden
    - UDP - een alternatief voor het TCP-protocol
- ***Lokaal adres*** - IP-adres en het gebruikte poortnummer van de lokale computer
- ***Extern adres*** - IP-adres en poortnummer van de externe computer waarmee een verbinding bestaat Zo mogelijk wordt ook de hostnaam van de externe computer opgezocht.
- ***Status*** - de meest waarschijnlijke huidige status (*Verbonden, Server moet worden afgesloten, Luisteren, Actieve afsluiting voltooid, Passieve afsluiting, Actieve afsluiting*)

Voor een lijst met alleen externe verbindingen, schakelt u het selectievakje ***Lokale verbindingen verbergen*** in het onderste deel van het dialoogvenster onder de lijst, in.

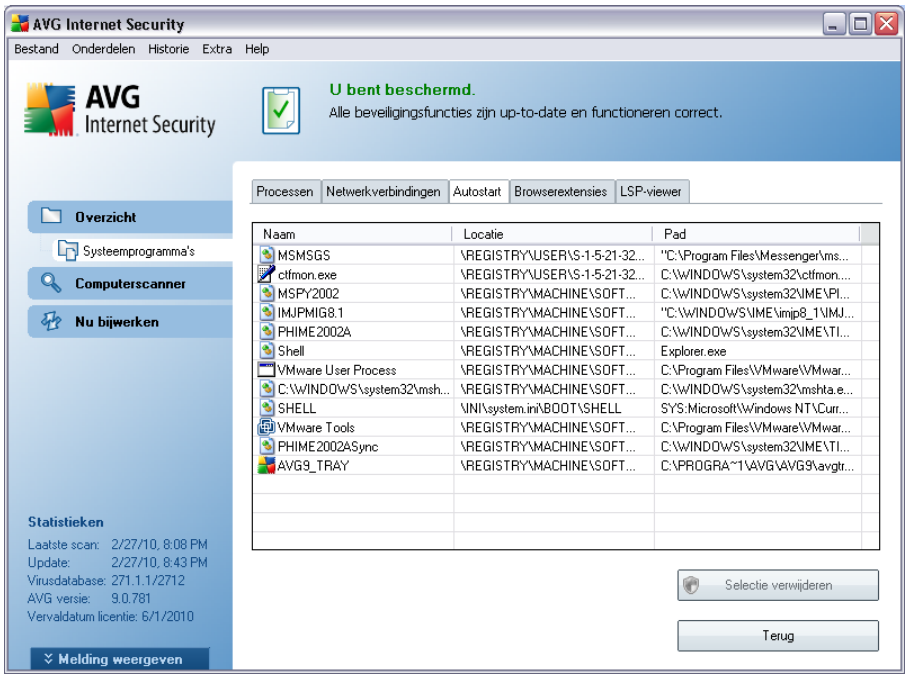
Knoppen

De beschikbare knoppen zijn:

- ***Verbinding beëindigen*** - één of meer geselecteerde verbindingen in de lijst worden verbroken
- ***Proces beëindigen*** - hiermee sluit u een of meer toepassingen die betrekking hebben op de in de lijst geselecteerde verbindingen
- ***Terug*** - terugkeren naar de standaard***AVG-gebruikersinterface*** (Overzicht van onderdelen).

Soms is het alleen mogelijk om toepassingen te beëindigen die momenteel de status Verbonden hebben. Het beëindigen van verbindingen raden we u ten zeerste af, tenzij u absoluut zeker weet dat deze verbindingen een bedreiging vormen!

8.5.3. Autostart

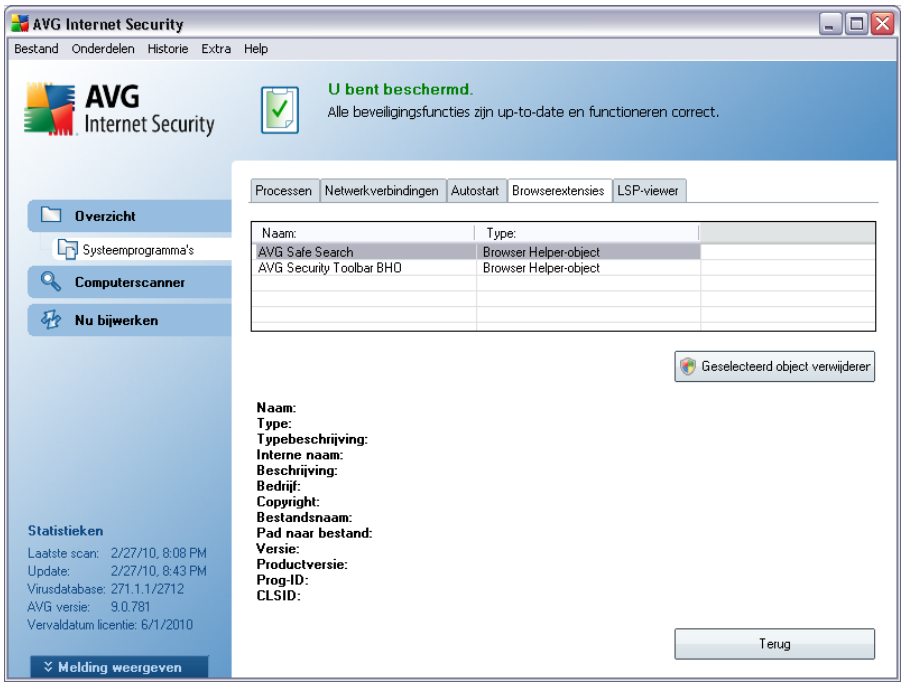


In het dialoogvenster ***Autostart*** staat een lijst met alle toepassingen die worden gestart bij het opstarten van Windows. Vaak voegen meerdere malware-toepassingen zichzelf automatisch toe aan het item in het opstartregister.

U kunt een of meer items verwijderen door deze te selecteren en op de knop ***Selectie verwijderen*** te klikken. Als u op de knop ***Terug*** klikt, keert u terug naar de standaard ***AVG-gebruikersinterface*** (Overzicht van onderdelen).

Het verwijderen van toepassingen uit de lijst raden we u ten zeerste af, tenzij u absoluut zeker weet dat deze toepassingen een bedreiging vormen!

8.5.4. Browserextensies



In het dialoogvenster ***Browserextensies*** staat een lijst met invoegtoepassingen (*bijvoorbeeld toepassingen*) die zijn geïnstalleerd in uw internetbrowser. Deze lijst kan invoegtoepassingen bevatten voor reguliere toepassingen maar ook potentiële malware-programma's. Klik op een object in de lijst voor gedetailleerde informatie over de geselecteerde invoegtoepassing, die in het onderste deel van het dialoogvenster wordt weergegeven.

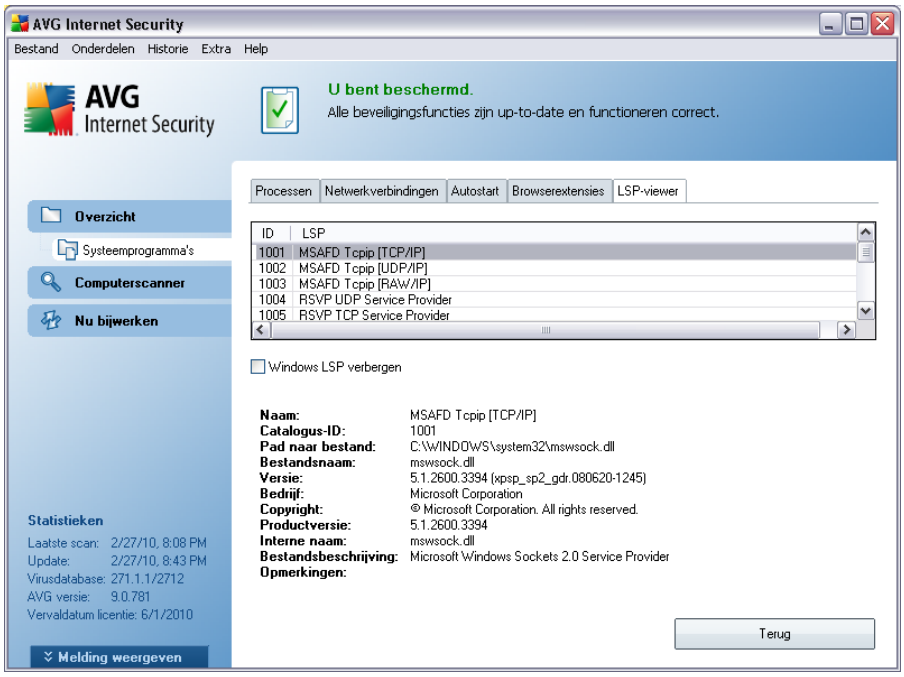
Knoppen

Op het tabblad ***Browserextensies*** staan de volgende knoppen:

- ***Geselecteerd object verwijderen*** - de op dat moment in de lijst geselecteerde invoegtoepassing verwijderen. ***Het verwijderen van invoegtoepassingen uit de lijst raden we u ten zeerste af, tenzij u absoluut zeker weet dat deze een reële bedreiging vormen!***

- ***Terug*** - als u op deze knop klikt, keert u terug naar de standaard ***AVG-gebruikersinterface*** (Overzicht van onderdelen)

8.5.5. LSP-viewer



In het dialoogvenster ***LSP-viewer*** staat een lijst met Layered Service Providers (LSP).

Een ***Layered Service Provider*** (LSP) is een systeemstuurprogramma dat is gekoppeld aan de netwerkservices van het Windows-besturingssysteem. Het verschaft toegang tot alle gegevens die de computer binnenkomen en verlaten, en kan deze gegevens ook wijzigen. Sommige LSP's zijn nodig om Windows een verbinding met andere computers te kunnen laten maken, waaronder een verbinding met het internet. Bepaalde malware-toepassingen kunnen zichzelf echter ook installeren als een LSP, waardoor zij toegang hebben tot alle gegevens die door uw computer worden verzonden. Aan de hand van deze lijst kunt u dus alle mogelijke bedreigingen van LSP's controleren.

Soms is het ook mogelijk om defecte LSP's te herstellen (*bijvoorbeeld wanneer het bestand is verwijderd maar de registerwaarden intact zijn gebleven*). Zodra een herstelbare LSP wordt aangetroffen, wordt een nieuwe knop voor reparatie van deze kwestie weergegeven.

Als u Windows LSP's in de lijst wilt opnemen, schakelt u het selectievakje ***Windows-LSP verbergen*** uit. Als u op de knop ***Terug*** klikt, keert u terug naar de standaard ***AVG-gebruikersinterface*** (*Overzicht van onderdelen*).

8.6. Firewall

Een firewall is een systeem dat een toegangsbeleid afdwingt tussen twee of meer netwerken door verkeer te blokkeren/toe te staan. Elke firewall heeft 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 dan toegestaan of verboden. Als de firewall inbreukpogingen herkent, wordt de poging geblokkeerd en krijgt de inbreker geen toegang tot de computer.

De Firewall wordt geconfigureerd voor het toestaan of blokkeren van interne/externe communicatie (in beide richtingen, naar binnen en naar buiten) door opgegeven poorten, en voor opgegeven software. De 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 zou dan worden geblokkeerd.

De Firewall beschermt uw persoonsgebonden informatie en verhindert dat die vanaf uw computer wordt verzonden zonder uw toestemming. De Firewall bepaalt hoe uw computer gegevens met andere computers op internet of in een lokaal netwerk uitwisselt. Binnen een organisatie beschermt de Firewall ook afzonderlijke computers tegen aanvallen die door interne gebruikers op andere computers in het netwerk worden uitgevoerd.

Aanbeveling: *Over het algemeen is het niet raadzaam om meer dan één firewall op een individuele 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 dat u slechts één firewall op uw computer gebruikt en alle andere firewalls deactiveert om zo het risico op mogelijke conflicten en hiermee verbonden problemen voorkomt.*

8.6.1. Firewallprincipes

In AVG bewaakt het onderdeel ***Firewall*** al het verkeer op elke netwerkpoort van uw computer. Op basis van de gedefinieerde regels worden met ***Firewall*** toepassingen geëvalueerd die worden uitgevoerd op de computer (en die u wilt verbinden met het Internet/het lokale netwerk) of toepassingen die de computer van buitenaf benaderen om verbinding te maken met de pc. Voor al deze toepassingen wordt via ***Firewall*** bepaald of de communicatie op de netwerkpoorten is toegestaan of verboden. Standaard zal ***Firewall*** u bij een onbekende toepassing (dat wil zeggen een toepassing waarvoor geen ***Firewall*** -regels zijn gedefinieerd) vragen of u communicatie wilt toestaan of blokkeren.

Opmerking: *AVG Firewall is niet bedoeld voor serverplatforms!*

Wat AVG Firewall kan doen:

- Communicatiepogingen van bekende toepassingen automatisch toestaan of blokkeren, of u vragen om bevestiging
- Volledige profielen gebruiken met vooraf gedefinieerde regels, naar uw wensen
- Overschakelen tussen profielen, automatisch bij de verbinding met verschillende soorten netwerken, of de toepassing van verschillende netwerkadapters

8.6.2. Firewallprofielen

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

Beschikbare profielen

- ***Alles toestaan*** - een ***firewall***-systeemprofiel dat vooraf is ingesteld door de fabrikant en altijd beschikbaar is. Als dit profiel wordt geactiveerd, wordt al het netwerkverkeer toegestaan en worden geen beveiligingsregels toegepast, alsof ***Firewall*** is uitgeschakeld *(alle toepassingen zijn bijvoorbeeld toegestaan, maar de pakketten worden niettemin gecontroleerd - als u alle vormen van filteren wilt uitschakelen, moet u Firewall echt uitschakelen)*. U kunt dit systeemprofiel niet dupliceren of verwijderen en u kunt de instellingen niet wijzigen.
- ***Blokkeer alles*** - een ***firewall***-systeemprofiel dat vooraf is ingesteld door de fabrikant en altijd beschikbaar is. Als dit profiel wordt geactiveerd, wordt al het netwerkverkeer geblokkeerd en is de computer vanuit netwerken van buitenaf niet toegankelijk en kan hij evenmin met de buitenwereld communiceren. U kunt dit systeemprofiel niet dupliceren of verwijderen en u kunt de instellingen niet wijzigen.
- ***Aangepaste profielen***:
    - ***Rechtstreeks verbonden met internet*** - geschikt voor gewone bureaucomputers thuis die rechtstreeks verbinding maken met internet,

en voor notebooks die verbinding maken met internet buiten het veilige bedrijfsnetwerk. Selecteer deze optie als u vanuit thuis verbinding maakt, of als u werkt in een klein bedrijfsnetwerk zonder echt centraal beheer. Selecteer bovendien deze optie als u op reis bent en verbinding maakt met uw notebook vanaf verschillende onbekende en mogelijk gevaarlijke plekken (*internetcafé, hotelkamer, enzovoort*). Er worden strengere regels gecreëerd, omdat er wordt aangenomen dat deze computers verder geen bescherming hebben en dus zo goed mogelijk beschermd moeten worden.

- ***Computer in een domain*** - geschikt voor computers in een lokaal netwerk, bijvoorbeeld het netwerk van een school of een bedrijfsnetwerk. Er wordt van uitgegaan dat het netwerk wordt beveiligd met aanvullende maatregelen, zodat een minder hoog beveiligingsniveau vereist is dan bij standalone computers.

- ***Klein thuis- of kantoornetwerk*** - geschikt voor computers in een klein netwerk, bijvoorbeeld thuis of in een klein bedrijf, waar slechts een paar computers met elkaar verbonden zijn, zonder "centrale" beheerder.

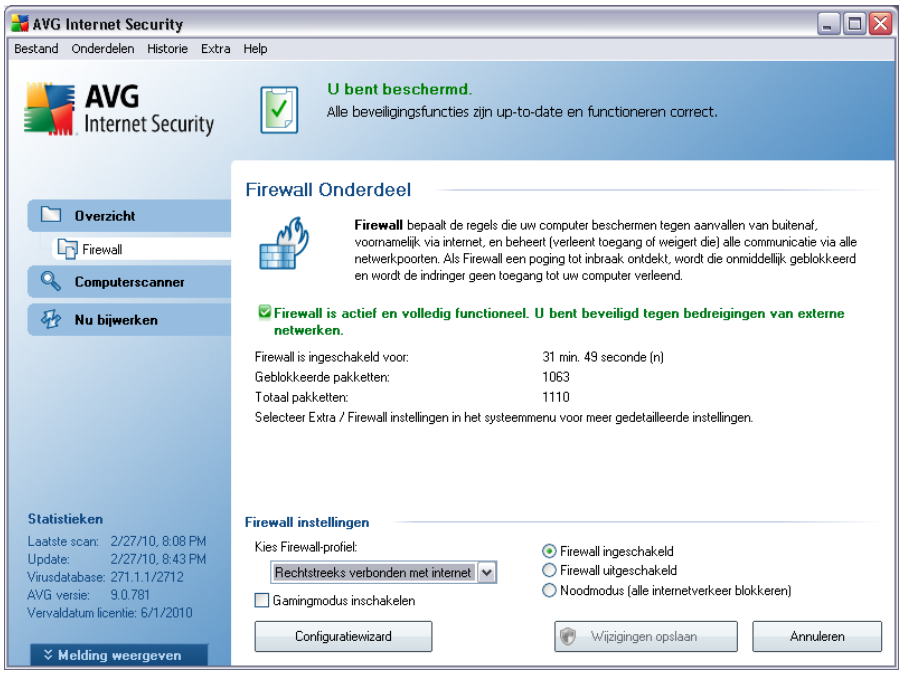
Profiel omschakelen

Via de functie Profiel omschakelen kan de ***Firewall*** automatisch omschakelen naar het gedefinieerde profiel wanneer u een bepaalde netwerkadapter gebruikt of wanneer u bent verbonden met een bepaald type netwerk. Als aan een netwerkgebied nog geen profiel is toegewezen, zal ***Firewall*** bij de eerstvolgende keer dat een verbinding tot stand wordt gebracht met dat gebied, een dialoogvenster openen met de vraag een profiel toe te wijzen.

U kunt profielen toewijzen aan alle lokale netwerkinterfaces en -gebieden en nadere instellingen opgeven in het dialoogvenster ***Profielen van gebieden en adapters***; in dat dialoogvenster kunt u de functie ook uitschakelen als u er geen gebruik van wilt maken.*dan zal voor alle typen verbindingen het standaardprofiel worden gebruikt*).

Gewoonlijk vinden gebruikers met een notebook die afhankelijk zijn van veel verschillende verbindingen, dit een handige functie. Als u een desktop computer hebt en steeds van dezelfde verbinding gebruikmaakt (*bijvoorbeeld een kabelverbinding met internet*), hoeft u geen aandacht te schenken aan het omschakelen van profielen, omdat u de functie waarschijnlijk nooit gebruikt.

8.6.3. Firewallinterface



De interface van het onderdeel ***Firewall*** biedt elementaire informatie over de functionaliteit van het onderdeel en een beknopt overzicht van ***Firewall*** statistieken:

- ***Firewall is ingeschakeld voor*** - Het tijdsverloop sinds de inschakeling van Firewall
- ***Geblokkeerde pakketten*** - het aantal geblokkeerde pakketten, afgezet tegen het totaal aan gecontroleerde pakketten
- ***Totaal pakketten*** - het totale aantal pakketten dat tijdens uitvoering van Firewall is gecontroleerd

Basisconfiguratie van het onderdeel

- ***Kies Firewall-profiel*** - selecteer in het vervolgkeuzemenu een van de gedefinieerde profielen - er zijn altijd twee profielen beschikbaar (de *standaardprofielen* ***Alles toestaan*** *en* ***Blokkeer alles***); daaraan hebt u andere profielen toegevoegd door profielen te wijzigen in het dialoogvenster ***Profielen*** van ***Firewall-instellingen***.

- ***Gamingmodus inschakelen*** - Schakel deze optie in, zodat u zeker weet dat bij uitvoering van schermvullende toepassingen (spelletjes, PowerPoint-presentaties, enz.), de ***Firewall*** geen dialoogvensters zal openen waarin u wordt gevraagd of u communicatie voor onbekende toepassingen al dan niet wilt toestaan. Als een onbekende toepassing op dat moment probeert te communiceren via het netwerk, zal de ***Firewall*** de poging toestaan of blokkeren, op basis van de instellingen in het huidige profiel.

- ***Firewallstatus***:

  - ***Firewall ingeschakeld*** - selecteer deze optie om communicatie toe te staan aan die toepassingen waarvoor 'toegestaan' is ingesteld in de set regels gedefinieerd voor het geselecteerde ***Firewall***-profiel

  - ***Firewall uitgeschakeld*** - met deze optie schakelt u ***Firewall*** helemaal uit; alle netwerkverkeer is toegestaan en er wordt niet gecontroleerd!

  - ***Alarmmodus (al het internetverkeer blokkeren)*** - met deze optie blokkeert u al het verkeer via alle netwerkpoorten; ***Firewall*** is weliswaar actief, maar al het netwerkverkeer is stilgelegd

Opmerking: *De leverancier heeft alle onderdelen van AVG zo ingesteld dat ze optimaal presteren. Wijzig de configuratie van AVG niet, tenzij er een goede reden is om dat wel te doen. Wijzigingen in de instellingen dienen alleen te worden uitgevoerd door ervaren gebruikers. Als de noodzaak voor wijziging van de configuratie van Firewall zich voordoet, selecteert u in het systeemmenu de optie* ***Extra / Firewall-instellingen*** *en wijzigt u de Firewallconfiguratie in het dialoogvenster* ***Firewall-instellingen*** *dat dan wordt geopend.*

Knoppen

- ***Configuratiewizard*** - klik op de knop om over te schakelen naar het desbetreffende dialoogvenster (*gebruikt in het installatieproces*) genaamd ***Instellingen computergebruik*** waarin u de configuratie voor de ***Firewall***kunt opgeven

- ***Wijzigingen opslaan*** - klik op deze knop om de wijzigingen die u in het dialoogvenster hebt uitgevoerd op te slaan en toe te passen

- ***Annuleren*** - klik op deze knop om terug te keren naar de standaard AVG-gebruikersinterface (*het overzicht van onderdelen*)

8.7. 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 daar zelden anti-spamtechnologie 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 e.d. in om de risico's in te dammen.

8.7.1. E-mailscanner principes

Het onderdeel ***E-mailscanner*** scant automatisch binnenkomende en uitgaande e-mails. U kunt E-mailscanner gebruiken voor e-mailclients die geen eigen invoegtoepassing hebben in AVG (*bijvoorbeeld Outlook Express, Mozilla, Incredimail, enzovoort*).

Bij de installatie van AVG worden automatische servers gecreëerd voor controle van e-mail: één voor het controleren van binnenkomende e-mail en één voor het controleren van uitgaande e-mails. Met behulp van deze twee servers worden e-mails automatisch gecontroleerd op poorten 110 en 25 (*standaardpoorten voor het versturen/ontvangen van e-mails*).

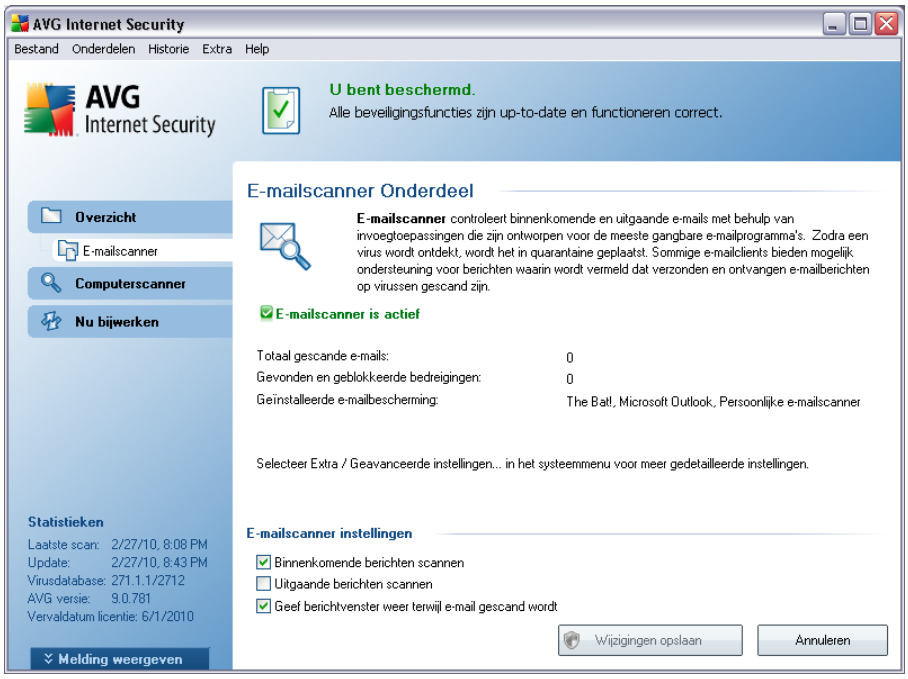
Persoonlijke e-mailscanner werkt als een interface tussen e-mailclient en e-mailservers op internet.

- ***Binnenkomende e-mail:*** als een bericht binnenkomt van de server, wordt het door het onderdeel ***E-mailscanner*** getest op virussen, worden geïnfecteerde bijlagen verwijderd, en wordt aan het bericht een certificaat gekoppeld. Bij detectie worden virussen meteen geïsoleerd in de ***Quarantaine***. Vervolgens wordt het bericht doorgestuurd naar de e-mailclient.

- ***Uitgaande e-mail:*** het bericht wordt door de e-mailclient verstuurd naar de E-mailscanner; daar wordt het bericht met de bijlagen gescand op virussen, waarna het naar de SMTP-server wordt gestuurd (*scannen van uitgaande e-mail is standaard uitgeschakeld, maar kan handmatig worden ingesteld*

Opmerking: *AVG E-mailscanner is niet bedoeld voor serverplatforms!*

8.7.2. E-mailscanner interface



Op het scherm van het onderdeel ***E-mailscanner*** staat een korte tekst met een beschrijving van de functie van het onderdeel, informatie over de huidige status (*E-mailscanner is actief.*) en de volgende statistieken:

- ***Totaal gescande e-mails:*** - het aantal gescande e-mailberichten sinds de laatste keer dat ***E-mailscanner*** is gestart (*desgewenst kan deze waarde opnieuw worden ingesteld, bijvoorbeeld voor statistische doeleinden - Waarde opnieuw instellen*)
- ***Gevonden en geblokkeerde bedreigingen*** - het aantal in e-mailberichten gedetecteerde infecties sinds de laatste keer dat ***E-mailscanner*** is gestart
- ***Geïnstalleerde e-mailbescherming*** - informatie over een specifieke invoegtoepassing voor e-mailbescherming die verwijst naar uw standaard e-mailclient

Basisconfiguratie van het onderdeel

In het onderste deel van het dialoogvenster is een sectie***Instellingen voor E-mailscanner*** waar u instellingen kunt opgeven voor een aantal elementaire functies

van het onderdeel:

- ***Binnenkomende berichten scannen*** - schakel het selectievakje bij deze optie in om op te geven dat alle e-mailberichten die aan uw account zijn ge richt, moeten worden gescand op virussen. Standaard is deze optie ingeschakeld en het wordt aanbevolen deze niet uit te schakelen.

- ***Uitgaande berichten scannen*** - schakel het selectievakje bij deze optie in om op te geven dat alle e-mailberichten die via uw account worden verzonden, moeten worden gescand op virussen. De optie is standaard uitgeschakeld.

- ***Waarschuwingspictogram weergeven bij het scannen van e-mail*** - schakel deze optie in als u informatie wilt krijgen via een waarschuwingspictogram dat over het AVG-pictogram in het systeemvak wordt weergegeven tijdens het scannen van uw mail met het onderdeel ***E-mailscanner***. Standaard is de optie ingeschakeld en het wordt aanbevolen deze niet uit te schakelen.

U kunt het dialoogvenster voor geavanceerde configuratie van ***E-mailscanner*** openen met de optie ***Extra/Geavanceerde instellingen*** in het systeemmenu; geavanceerde configuratie wordt echter alleen aangeraden voor ervaren computergebruikers!

Opmerking: *De leverancier heeft alle onderdelen van AVG zo ingesteld dat ze optimaal presteren. Wijzig de configuratie van AVG niet, tenzij er een goede reden is om dat wel te doen. Wijzigingen in de instellingen dienen alleen te worden uitgevoerd door ervaren gebruikers. Als u de AVG-configuratie dient te wijzigen, selecteert u in het systeemmenu de optie****Tools / Geavanceerde instellingen*** *en bewerkt u de AVG-configuratie in het nieuw geopende dialoogvenster AVG Geavanceerde instellingen.*

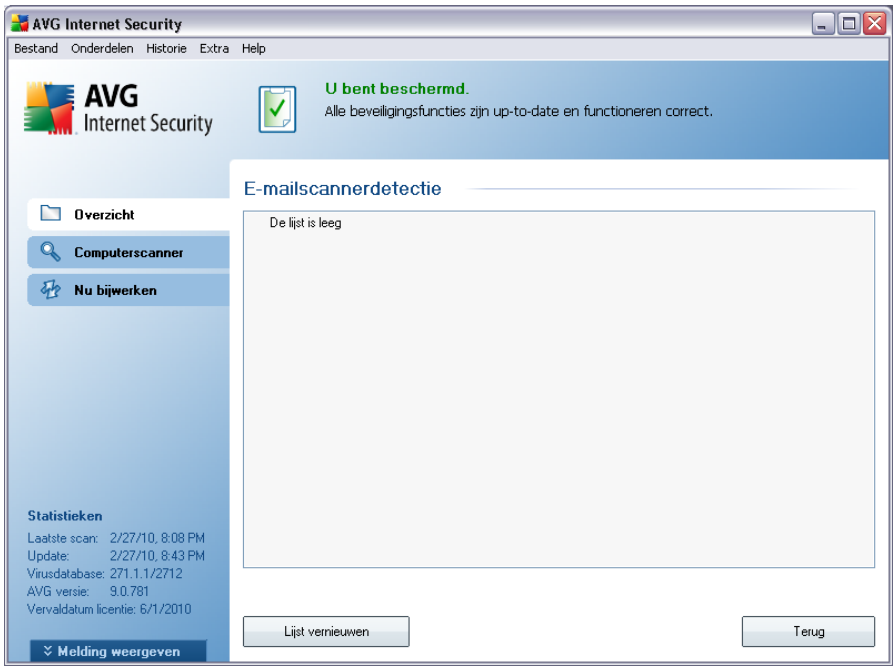
Knoppen

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

- ***Wijzigingen opslaan*** - klik op deze knop om de wijzigingen die u in het dialoogvenster hebt uitgevoerd op te slaan en toe te passen

- ***Annuleren*** - klik op deze knop om het dialoogvenster te sluiten zonder wijzigingen op te slaan, en terug te keren naar de standaard AVG-gebruikersinterface (het overzicht van onderdelen)

8.7.3. E-mailscanner detectie



Het dialoogvenster ***E-mailscannerdetectie*** (*dat u opent door in het hoofdmenu de optie Historie / E-mailscannerdetectie te kiezen*) bevat een lijst met alle door het onderdeel ***E-mailscanner***gedetecteerde items. Bij elk object wordt de volgende informatie weergegeven:

- ***Infectie*** - beschrijving (indien mogelijk de naam) van het gedetecteerde object
- ***Object*** - locatie van het object
- ***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

In het onderste gedeelte van het dialoogvenster, onder de lijst, vindt u informatie over het totale aantal gedetecteerde objecten dat hierboven wordt weergegeven. Bovendien kunt u de hele lijst met gedetecteerde objecten exporteren naar een bestand (***Lijst exporteren naar een bestand***) en alle invoer 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
- ***Terug*** - als u op deze knop klikt, keert u terug naar de standaard ***AVG-gebruikersinterface*** (Overzicht van onderdelen)

8.8. ID Protection

AVG Identity Protection is een anti-malwareproduct dat zich richt op preventie van diefstal van uw wachtwoorden, bankrekeninggegevens, creditcardnummers en andere persoonlijke digitale waardevolle 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. ***AVG Identity Protection*** werkt door doorlopend verdacht gedrag te detecteren en te blokkeren en beschermt uw computer tegen alle nieuwe schadelijke software.

8.8.1. ID Protection principes

AVG Identity Protection is een onderdeel voor anti-malware dat u beschermt tegen allerlei vormen van malware (*zoals spyware, bots en identiteitsdiefstal, enz.*) via gedragsherkennende technologieën, en dat zonder enige vertraging bescherming biedt tegen nieuwe virussen. Malware wordt steeds meer geperfectioneerd en neemt de vorm van normale programma's aan die uw computer blootstellen aan externe aanvallen van identiteitsdiefstal. Met ***AVG Identity Protection*** bent u beschermd tegen deze vorm van schadelijke uitvoerbare malwarebestanden. Het is een vorm van aanvullende bescherming op ***AVG Anti-Virus,*** dat u beschermt tegen virussen in bestanden en bekende virussen met behulp van handtekeningenmechanismen en scanprocedures.

We raden u met nadruk aan om zowel AVG Anti-Virus als AVG Identity Protection te installeren om uw pc volledig te beschermen.

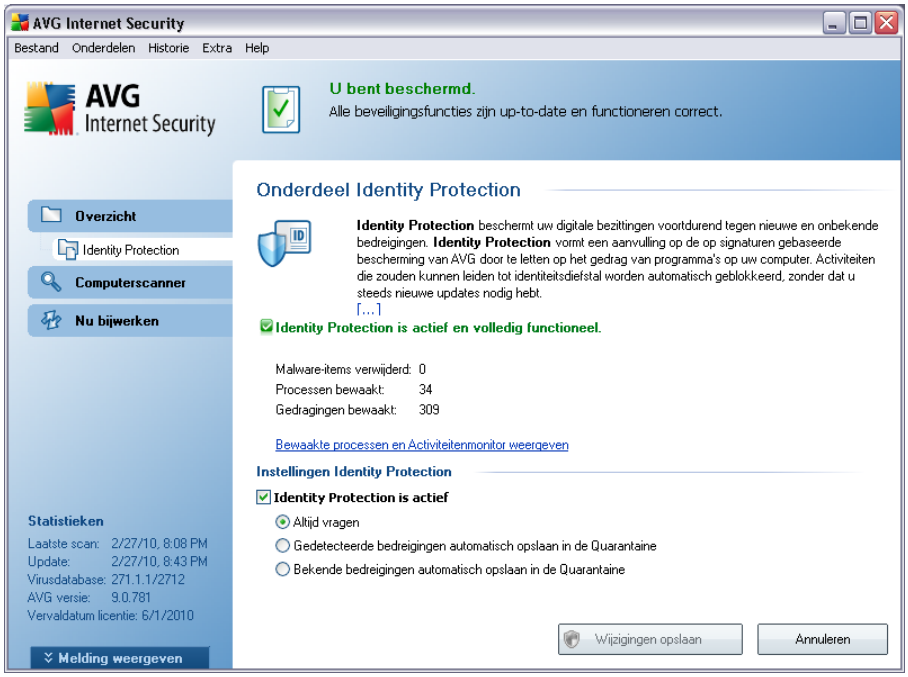
8.8.2. ID Protection interface

De gebruikersinterface van ***Identity Protection*** biedt een korte beschrijving van de functionaliteit van het onderdeel, informatie over de huidige status van het onderdeel (*AVG Identity Protection is actief en volledig functioneel.*) en enige statistische cijfers:

- ***Malware-items verwijderd*** - het aantal toepassingen dat is gedetecteerd als malware en is verwijderd

- ***Bewaakte processen*** - het aantal toepassingen dat op dat moment wordt uitgevoerd en wordt bewaakt door IDP

- ***Bewaakte gedragingen*** - het aantal specifieke acties dat in de bewaakte toepassingen wordt uitgevoerd



Basisconfiguratie van het onderdeel

In het onderste deel van het dialoogvenster is een sectie ***Instellingen voor Identity Protection*** waar u instellingen kunt opgeven voor een aantal elementaire functies van het onderdeel:

- ***Identity Protection is actief*** - (*standaard ingeschakeld*) schakel het selectievakje in om het onderdeel IDP in te schakelen en meer opties weer te geven voor instellingen.

Het kan voorkomen dat ***Identity Protection*** een legitiem bestand als verdacht of gevaarlijk rapporteert. Aangezien ***Identity Protection*** bedreigingen herkent op grond van hun gedrag, treedt dit probleem meestal op wanneer een programma toetsaanslagen opslaat of andere programma's installeert, of wanneer er een nieuw stuurprogramma op de computer wordt geïnstalleerd.

Maak daarom een keuze uit één van de volgende manieren waarop ***Identity***

Protection kan reageren als er verdachte activiteiten worden gedetecteerd:

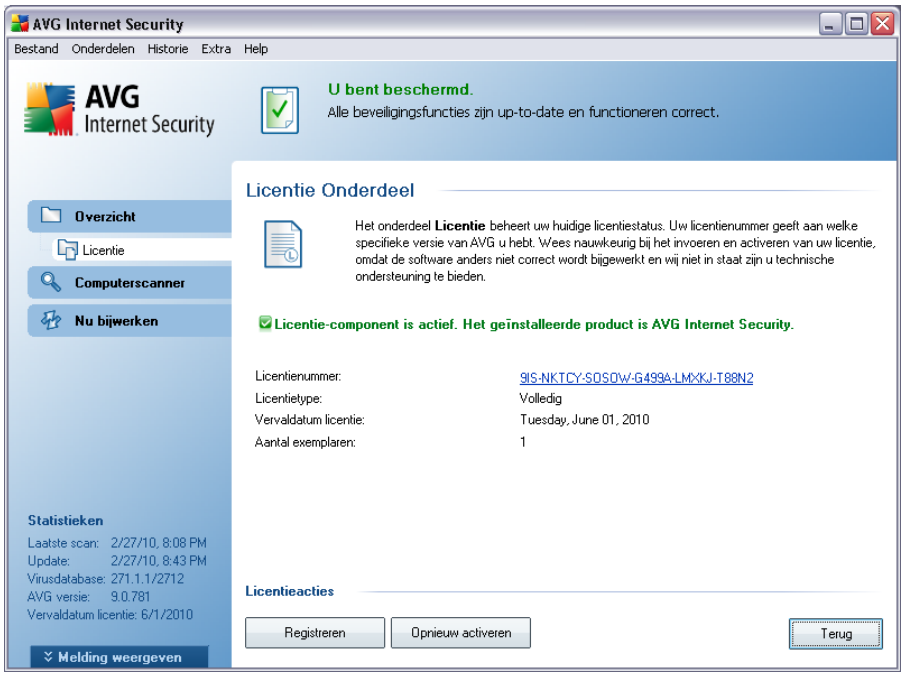
- ***Altijd vragen*** - als een toepassing wordt herkend als malware, wordt u gevraagd of de toepassing moet worden geblokkeerd (*de optie is standaard ingeschakeld en we raden u aan deze niet te wijzigen, tenzij u een goede reden heeft om dit wel te doen*)
- ***Gedetecteerde bedreigingen automatisch opslaan in de Quarantaine*** - alle toepassingen die worden herkend als malware worden automatisch geblokkeerd
- ***Bekende bedreigingen automatisch opslaan in de Quarantaine*** - alleen toepassingen waarvan het absoluut zeker is dat het om malware gaat, zullen worden geblokkeerd

Knoppen

De interface van ***Identity Protection*** heeft de volgende knoppen:

- ***Wijzigingen opslaan*** - klik op deze knop om de wijzigingen die u in het dialoogvenster hebt uitgevoerd op te slaan en toe te passen
- ***Annuleren*** - klik op deze knop om het dialoogvenster te sluiten zonder wijzigingen op te slaan, en terug te keren naar de standaard AVG-gebruikersinterface (het overzicht van onderdelen)

8.9. Licentie



Op het scherm van het onderdeel ***Licentie*** staat een korte tekst met een beschrijving van de functionaliteit van het onderdeel, informatie over de huidige status (*Licentie-component is actief.*) en de volgende informatie:

- ***Licentienummer*** - de exacte vorm van het licentienummer. Als u uw licentienummer invoert, dient u het heel nauwkeurig zo te typen als het wordt weergegeven. We raden u dan ook met nadruk aan bij alle bewerkingen met het licentienummer de "knippen-en-plakken"-methode toe te passen.
- ***Licentietype*** - het type geïnstalleerd product.
- ***Vervaldatum licentie*** - de datum waarop de licentie zijn geldigheid verliest. Als u na die datum **AVG 9 Internet Security** wilt blijven gebruiken, zult u de licentie moeten vernieuwen. U kunt de licentie online vernieuwen op de website van AVG (http://www.avg.com/).
- ***Aantal exemplaren*** - het aantal werkstations waarop u **AVG 9 Internet Security** mag installeren.

Knoppen

- ***Registreren*** - verbinding maken met de registratiepagina van de website van AVG (http://www.avg.com/). Voer uw registratiegegevens in; alleen klanten die hun AVG product registreren komen in aanmerking voor gratis technische ondersteuning.

- ***Opnieuw activeren*** - het dialoogvenster ***AVG activeren*** wordt geopend met de gegevens die u hebt opgegeven in het dialoogvenster ***AVG aanpassen*** van de installatieprocedure. In dit dialoogvenster kunt u uw licentienummer invoeren ter vervanging van ofwel het verkoopnummer (*het nummer waarmee u AVG heeft geïnstalleerd*), ofwel het oude licentienummer (*bijvoorbeeld bij het upgraden naar een nieuw product van AVG*).

Opmerking: Als u de proefversie van *AVG 9 Internet Security* **gebruikt, worden de knoppen weergegeven als** *Nu kopen* ***en*** *Activeren, zodat u de volledige versie van het programma meteen kunt kopen. Als u* **AVG 9 Internet Security** *hebt geïnstalleerd met een verkoopnummer, worden deze knoppen weergegeven als* ***Registreren*** *en* ***Activeren****.*

- ***Terug*** - klik op deze knop om terug te keren naar de standaard AVG gebruikersinterface (het overzicht van onderdelen).

8.10. LinkScanner

8.10.1. LinkScanner principes

AVG LinkScanner biedt bescherming tegen websites die worden ontwikkeld om malware op uw computer te installeren via de webbrowser of invoegtoepassingen van de webbrowser. De ***LinkScanner***-technologie is verdeeld over twee functies, ***AVG Search-Shield*** en ***AVG Active Surf-Shield***:

- ***AVG Search-Shield***bevat een lijst met websites (*URL-adressen*) waarvan bekend is dat ze gevaarlijk zijn. Bij zoeken met Google, Yahoo!, Bing, Baidu, Altavista of Yandex worden alle resultaten van de zoekopdracht vergeleken met deze lijst en wordt er een beoordelingspictogram weergegeven (*voor Yahoo! wordt alleen een pictogram weergeven als het oordeel "website met exploit" luidt*). Ook als u rechtstreeks op de adresbalk van uw browser een adres typt, of op een koppeling op een webpagina klikt, of bijvoorbeeld in een e-mailbericht, wordt het adres automatisch gecontroleerd en zo nodig geblokkeerd.

- ***AVG Active Surf-Shield***scant de inhoud van webpagina's die u bezoekt, ongeacht het adres van de website. Zelfs als een verdachte website niet wordt gedetecteerd door ***AVG Search Shield*** (*bijvoorbeeld wanneer het om een nieuwe kwaadaardige website gaat, of als een website die eerder schoon was, nu besmet is met malware*), zal die website worden gedetecteerd en door ***AVG Active Surf-Shield*** worden geblokkeerd op het moment dat u de site probeert te bezoeken.

Opmerking: *AVG LinkScanner is niet bedoeld voor serverplatforms!*

8.10.2. Interface LinkScanner

Het onderdeel ***LinkScanner*** bestaat uit twee programmafuncties die u in en uit kunt schakelen in de interface van het ***Onderdeel LinkScanner***:

De interface van het onderdeel ***LinkScanner*** biedt een korte beschrijving van de functionaliteit van het onderdeel en informatie over de huidige status (*onderdeel LinkScanner is actief.*). Bovendien staat er informatie over het nieuwste versienummer van de ***LinkScanner***-database (|*LinkScanner-versie*).

In het onderste deel van het dialoogvenster kunt u verscheidene opties instellen:

- ***AVG Search-Shield inschakelen*** – (*standaard ingeschakeld*): pictogrammen

met een indicatie bij de resultaten van zoekopdrachten met Google, Yahoo!, Bing, Baidu, Yandex of Altavista die wordt verkregen door vooraf de inhoud van sites die door de zoekmachine worden geretourneerd, te controleren.

- ***AVG Active Surf-Shield inschakelen*** - (*standaard ingeschakeld*): actieve (*real-time*) bescherming tegen websites met exploits op het moment dat ze worden geadresseerd. Als zodanig bekend staande kwaadaardige sites en de inhoud met exploits worden geblokkeerd op het moment dat de gebruiker ze adresseert in de browser (*of met een andere toepassing die HTTP gebruikt*).

- ***Rapportage van gedetecteerde bedreigingen naar AVG inschakelen*** - schakel dit selectievakje in voor rapportage van exploits en kwaadaardige sites waarmee gebruikers via ***Safe Surf*** of ***Safe Search*** zijn geconfronteerd, naar de database waarin gegevens worden verzameld over kwaadaardige praktijken op internet.

8.10.3. AVG Search Shield

Als u op internet zoekt, terwijl ***AVG Search Shield*** is ingeschakeld, worden alle zoekresultaten van de belangrijkste zoekmachines zoals Yahoo!, Google, Bing, Altavista, Yandex, enz. weergegeven. beoordeeld op gevaarlijke of verdachte koppelingen. De ***AVG Link Scanner*** controleert deze koppelingen, markeert de slechte koppelingen en waarschuwt u zo voordat u op een gevaarlijke of verdachte koppeling klikt, zodat u zeker weet dat u alleen naar veilige websites gaat.

Terwijl een koppeling op de pagina met resultaten wordt beoordeeld, wordt bij die koppeling een pictogram weergegeven om aan te geven dat de beoordeling wordt uitgevoerd. Zodra de beoordeling is voltooid, wordt een pictogram ter aanduiding van de gevonden informatie weergegeven:

De gekoppelde pagina is veilig (*als u Yahoo! Search gebruikt met de AVG Werkbalk Beveiliging wordt dit pictogram niet weergegeven!*).

De gekoppelde pagina bevat geen bedreigingen, maar is enigszins verdacht (*of van twijfelachtige oorsprong of strekking en daarom niet geschikt voor e-shopping en dergelijke.*).

De gekoppelde pagina is zelf wellicht veilig, maar bevat misschien koppelingen naar pagina's die zonder meer gevaarlijk zijn of gevaarlijke code bevatten, ook al vormen ze op het moment nog geen bedreiging.

De gekoppelde pagina bevat actieve bedreigingen! U krijgt voor uw eigen bescherming geen toestemming de pagina te bezoeken.

De gekoppelde pagina is niet toegankelijk en is daarom niet gescand.

Als u de muisaanwijzer op een pictogram plaatst, worden details van de desbetreffende koppeling weergegeven. Die extra informatie betreft details van de dreiging (als die er is), het IP-adres van de pagina en het tijdstip waarop de pagina door AVG is gescand:

8.10.4. AVG Active Surf-Shield

Dit krachtige schild blokkeert de kwaadaardige inhoud van webpagina's die u probeert te openen en voorkomt dat die 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. Het is belangrijk te weten dat webpagina's met een exploit uw computer kunnen infecteren, alleen al als u de desbetreffende site bezoekt; om die reden zal de ***AVG LinkScanner*** verhinderen dat uw webbrowser gevaarlijke webpagina's met exploits of andere serieuze bedreigingen weergeeft.

Als u wordt geconfronteerd met een kwaadaardige website, wordt u door de ***AVG Link Scanner*** gewaarschuwd met een scherm als het volgende:

Bezoeken van een dergelijke website is zeer gevaarlijk en kan niet worden aanbevolen!

8.11. Online Shield

8.11.1. Online Shield principes

Online Shield is een vorm van interne, real-time 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 gaan bezoeken, bijvoorbeeld een gevaarlijk Javascript bevat, wordt weergave van die pagina verhinderd. Bovendien herkent het malware op pagina's en verhindert het onmiddellijk dat de malware wordt gedownload, zodat de malware uw computer nooit bereikt.

Opmerking: *AVG Online Shield is niet bedoeld voor serverplatforms!*

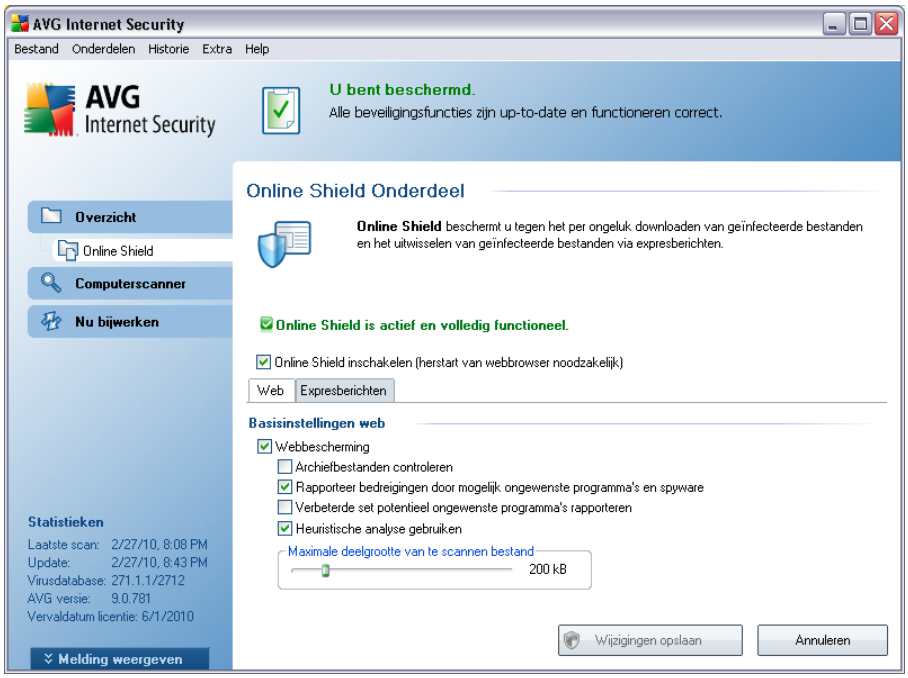
8.11.2. Online Shield interface

De interface van het onderdeel ***Online Shield*** beschrijft wat dit type bescherming doet. Bovendien vindt u er informatie over de huidige status van het onderdeel (*Online Shield is actief en volledig functioneel.*). In het onderste deel van het dialoogvenster staan de elementaire bewerkingsopties voor het functioneren van het onderdeel.

Basisconfiguratie van het onderdeel

Om te beginnen is er een optie waarmee u ***Online Shield*** kunt in- en uitschakelen met behulp van het selectievakje ***Online Shield inschakelen***. De optie is standaard ingeschakeld, zodat het onderdeel ***Online Shield*** actief is. We raden u aan om het onderdeel niet uit te schakelen, tenzij u een goede reden hebt om dat wel te doen. Als het selectievakje is ingeschakeld en ***Online Shield*** dus actief is, zijn er twee tabbladen met aanvullende opties voor configuratie:

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



- ***Webbescherming*** - met deze optie geeft u op of ***Online Shield*** de inhoud van webpagina's moet scannen. Ervan uitgaande dat deze optie (*standaard*) is ingeschakeld, kunt u nog de volgende functies in- en uitschakelen:

  - ***Archiefbestanden controleren*** - de inhoud van archieven scannen die zijn inbegrepen op de webpagina die u wilt weergeven

  - ***Bedreigingen door mogelijk ongewenste programma's en spyware rapporteren*** - (*standaard ingeschakeld*): schakel dit selectievakje in om de ***Anti-Spyware***-engine te activeren en naar spyware en virussen te scannen. Spyware behoort tot een twijfelachtige categorie malware en vormt gewoonlijk een veiligheidsrisico, maar sommige van deze programma's kunnen ook met opzet worden geïnstalleerd. Het is raadzaam deze functie niet uit te schakelen, omdat het de bescherming van uw computer vergroot

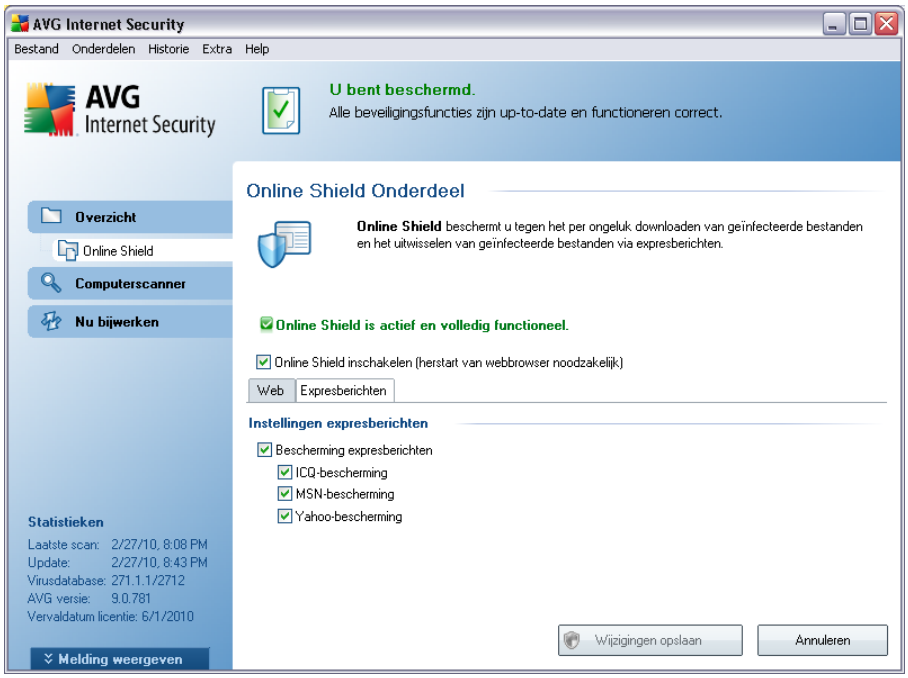
  - ***Uitgebreide sets van mogelijk ongewenste programma's rapporteren*** - als de vorige optie is geactiveerd, kunt u ook dit selectievakje inschakelen om uitgebreide pakketten van spyware te detecteren: programma's waar op zich niets aan mankeert als u ze direct van de fabrikant krijgt, maar die wel in een later stadium voor kwaadaardige praktijken kunnen worden misbruikt. 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.

- ***Heuristische methode gebruiken*** - de inhoud scannen van een weer te geven pagina met behulp van de methode voor heuristische analyse, dat wil zeggen simulatie en evaluatie van de instructies van het gescande object in een virtuele computeromgeving. Daarom kan door middel van heuristische analyse zelfs kwaadaardige code worden opgespoord die nog niet is beschreven in de virusdatabase).*(zie Anti-Virus principes*).

- ***Maximale grootte te scannen bestand*** - Als er bestanden zijn inbegrepen op een weer te geven pagina, kunt u de inhoud daarvan ook scannen voordat ze naar uw computer wrden gedownload. Het scannen van grote bestanden neemt echter soms veel tijd in beslag, wat het downloaden van de webpagina aanzienlijk kan vertragen. Met behulp van de schuifbalk 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: in het geval dat het bestand is geïnfecteerd, zal dat onmiddellijk worden gedetecteerd door ***Resident Shield***.

- ***Expresberichten*** - de instellingen voor het onderdeel opgeven die betrekking hebben op het scannen van expresberichten (*bijv. ICQ, MSN Messenger, Yahoo ...*).



o Bescherming expresberichten - schakel dit selectievakje in als u wilt dat Online Shield controleert of de online communicatie virusvrij is. Als de optie is ingeschakeld, kunt u nog opgeven welke toepassing voor expresberichten u wilt controleren - op dit moment ondersteunt **AVG 9 Internet Security** de toepassingen ICQ, MSN en Yahoo.

Opmerking: De leverancier van *heeft alle onderdelen van AVG zo ingesteld dat ze optimaal presteren. Wijzig de configuratie van AVG niet, tenzij er een goede reden is om dat wel te doen. Wijzigingen in de instellingen dienen alleen te worden uitgevoerd door ervaren gebruikers. Als u de AVG-configuratie dient te wijzigen, selecteert u in het systeemmenu de optie**Tools / Geavanceerde instellingen** en bewerkt u de AVG-configuratie in het nieuw geopende dialoogvenster AVG Geavanceerde instellingen.*

Knoppen

De interface van ***Online Shield*** heeft de volgende knoppen:

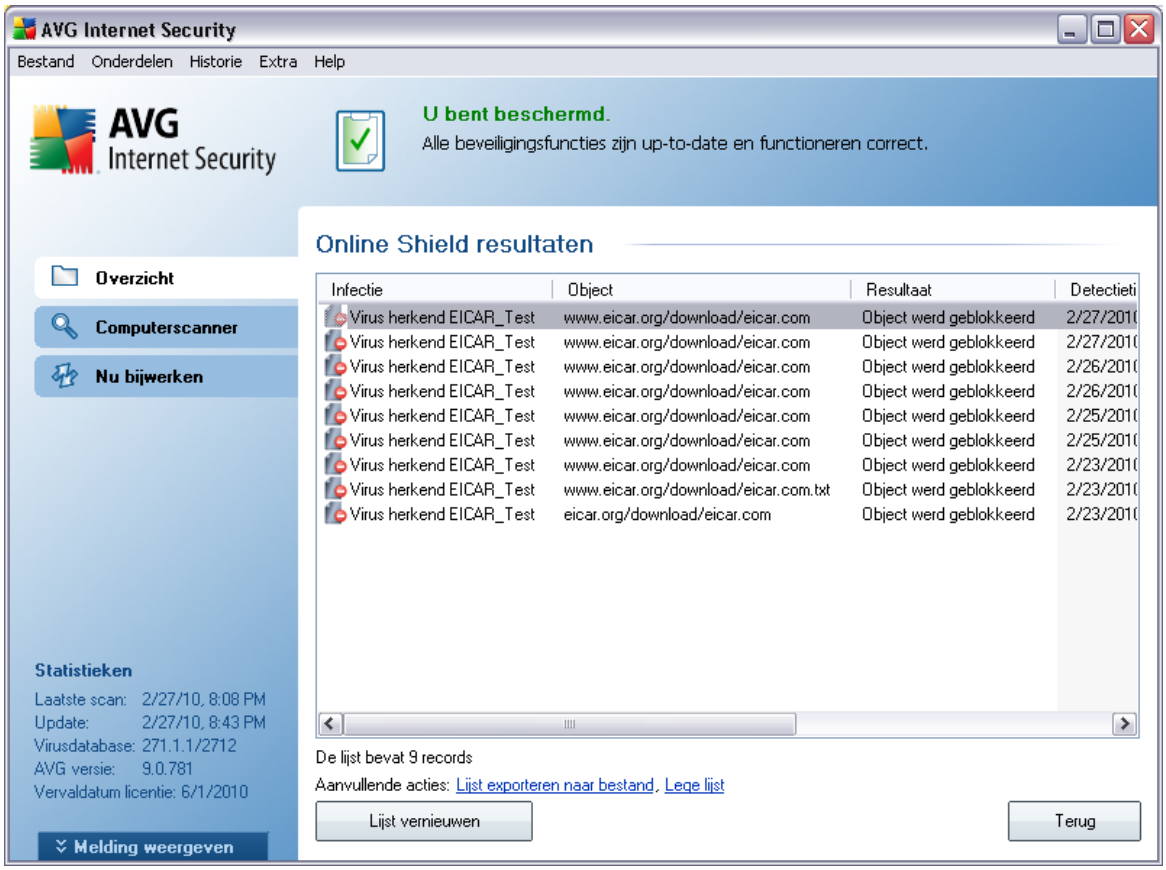
- ***Wijzigingen opslaan*** - klik op deze knop om de wijzigingen die u in het dialoogvenster hebt uitgevoerd op te slaan en toe te passen
- ***Annuleren*** - klik op deze knop om terug te keren naar de standaard AVG-

gebruikersinterface (*het overzicht van onderdelen*)

8.11.3. Online Shield detectie

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:

De verdachte webpagina wordt niet geopend en de gedetecteerde bedreiging wordt geregistreerd in de lijst met ***Online Shield resultaten*** - dit overzicht van gedetecteerde bedreigingen opent u door in het hoofdmenu de optie ***Historie / Online Shield resultaten*** te kiezen.



Bij elk object wordt de volgende informatie weergegeven:

- ***Infectie*** - beschrijving (*indien mogelijk de naam*) van het gedetecteerde object
- ***Object*** - bron van het object (*webpagina*)
- ***Resultaat*** - 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 hierboven wordt weergegeven. Bovendien kunt u de hele lijst met gedetecteerde objecten exporteren naar een bestand (***Lijst exporteren naar een bestand***) en alle invoer over gedetecteerde objecten wissen (***Lijst leegmaken***). Als u op de knop ***Lijst vernieuwen*** klikt, wordt de lijst met door ***Online Shield*** gedetecteerde items vernieuwd. Als u op de knop ***Terug*** klikt, keert u terug naar de standaard ***AVG-gebruikersinterface*** (Overzicht van onderdelen).

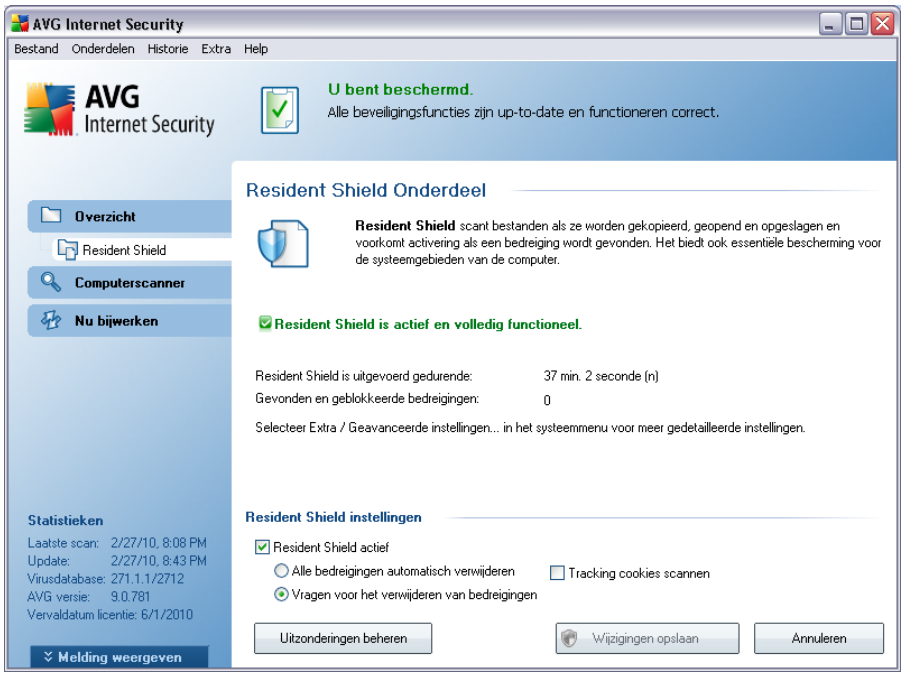
8.12. Resident Shield

8.12.1. Resident Shield Principes

Het onderdeel ***Resident Shield*** biedt uw computer permanente beveiliging.Resident Shield scant elk bestand dat wordt geopend, opgeslagen, of gekopieerd en bewaakt de systeemgebieden van de computer.Als ***Resident Shield*** een virus ontdekt in een bestand dat wordt geadresseerd, breekt het de bewerking die op dat moment wordt uitgevoerd, af en verhindert het dat het virus zichzelf activeert. Normaal gesproken merkt u niets van het proces, omdat het 'op de achtergrond' wordt uitgevoerd en u alleen wordt gewaarschuwd als er sprake is van bedreigingen; tegelijkertijd wordt dan door ***Resident Shield*** activering van de bedreiging geblokkeerd en wordt de bedreiging verwijderd. ***Resident Shield*** wordt in het geheugen van de computer geladen tijdens het opstarten van het systeem.

Waarschuwing: Resident Shield wordt in het geheugen van de computer geladen tijdens het opstarten; het is cruciaal dat u Resident Shield onder geen beding uitschakelt!

8.12.2. Resident Shield interface



Behalve een overzicht van de belangrijkste statistische gegevens en informatie over de huidige status van het onderdeel (*Resident Shield is actief en volledig functioneel*) heeft de interface van ***Resident Shield*** ook een paar opties voor het instellen van elementaire parameters voor het onderdeel. Het gaat om de volgende statistieken:

- ***Resident Shield is actief geweest voor*** - het tijdsverloop sinds de laatste keer dat het onderdeel is gestart
- ***Gevonden en geblokkeerde bedreigingen*** - het aantal gedetecteerde infecties waarvan uitvoering/openen is verhinderd (*u kunt deze waarde desgewenst opnieuw instellen, bijvoorbeeld voor statistische doeleinden - Waarde opnieuw instellen*)

Basisconfiguratie van het onderdeel

Onder in het dialoogvenster is een gedeelte ***Resident Shield instellingen***, waar u een paar basisinstellingen kunt opgeven voor het functioneren van het onderdeel (*voor gedetailleerde configuratie kiest u, net als voor alle andere onderdelen de optie Extra/ Geavanceerde instellingen in het systeemmenu*).

Met de optie ***Resident Shield is actief*** kunt u de bescherming door Resident Shield gemakkelijk in- en uitschakelen. Standaard is het onderdeel ingeschakeld. Als Resident Shield is ingeschakeld, kunt u nog nader specificeren hoe gedetecteerde infecties moeten worden verwijderd:

- automatisch (***Alle bedreigingen automatisch verwijderen***)
- of na bevestiging door de gebruiker (***Vragen voor het verwijderen van bedreigingen***)

Deze keuze heeft geen invloed op de mate van bescherming en komt alleen maar tegemoet aan uw voorkeur.

In beide gevallen kunt u kiezen voor ***Tracking cookies scannen***. Onder bepaalde omstandigheden kunt u deze optie inschakelen voor een maximale bescherming; standaard is de functie uitgeschakeld. (*Cookies zijn pakketjes tekst die door een server naar een webbrowser worden gestuurd, die steeds onveranderd door de webbrowser worden teruggestuurd op het moment dat de browser de server adresseert. HTTP-cookies worden gebruikt voor verificatie, tracking en het bijhouden van bepaalde informatie over gebruikers, bijvoorbeeld voorkeuren voor websites of de inhoud van winkelkarretjes*).

Opmerking: De leverancier van *heeft alle onderdelen van AVG zo ingesteld dat ze optimaal presteren. Wijzig de configuratie van AVG niet, tenzij er een goede reden is om dat wel te doen. Wijzigingen in de instellingen dienen alleen te worden uitgevoerd door ervaren gebruikers. Als u de AVG-configuratie dient te wijzigen, selecteert u in het systeemmenu de optie****Tools / Geavanceerde instellingen*** *en bewerkt u de AVG-configuratie in het nieuw geopende dialoogvenster AVG Geavanceerde instellingen.*

Knoppen

De interface van ***Resident Shield*** heeft de volgende knoppen:

- ***Uitzonderingen beheren*** - als u op deze knop klikt, wordt het dialoogvenster ***Uitsluitingen voor directory met Resident Shield*** geopend, waarin u mappen kunt opgeven die niet door ***Resident Shield*** moeten worden gescand
- ***Wijzigingen opslaan*** - klik op deze knop om de wijzigingen die u in het dialoogvenster hebt uitgevoerd op te slaan en toe te passen
- ***Annuleren*** - klik op deze knop om het dialoogvenster te sluiten zonder wijzigingen op te slaan, en terug te keren naar de standaard ***AVG-gebruikersinterface*** (het overzicht van onderdelen)

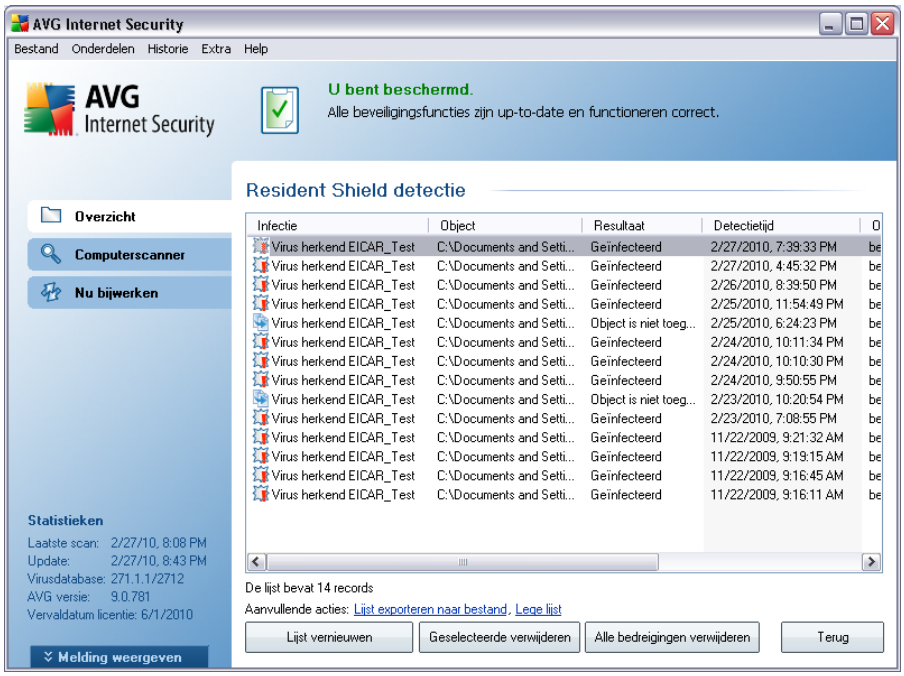
8.12.3. Resident Shield detectie

Resident Shield scant bestanden als ze worden gekopieerd, geopend of opgeslagen. Als een virus of een andere bedreiging wordt gedetecteerd, wordt u meteen gewaarschuwd door het volgende dialoogvenster:

In het dialoogvenster staat informatie over de gedetecteerde bedreiging; u kunt kiezen welke actie moet worden ondernomen:

- ***Herstellen*** - als het mogelijk is, zal AVG het geïnfecteerde bestand automatisch herstellen; dit is de aanbevolen actie
- ***Naar quarantaine verplaatsen*** - het virus zal worden verplaatst naar de AVG ***Quarantaine***
- ***Ga naar bestand*** - u wordt verwezen naar de exacte locatie van het verdachte object (*er wordt een nieuw Verkennervenster geopend*)
- ***Negeren*** - We raden u met nadruk aan deze optie NIET te kiezen tenzij u een heel goede reden hebt om dat wel te doen!

Het totale overzicht van alle bedreigingen die ***Resident Shield*** heeft gedetecteerd, is te vinden in het dialoogvenster ***Resident Shield detectie*** dat u opent door in het hoofdmenu de optie ***Historie / Resident Shield resultaten*** te kiezen:



In het dialoogvenster ***Resident Shield detectie*** staat een overzicht van objecten die door ***Resident Shield*** zijn gedetecteerd, beoordeeld en aangemerkt als gevaarlijk en vervolgens zijn hersteld of verplaatst naar de ***Quarantaine***. Bij elk object wordt de volgende informatie weergegeven:

- ***Infectie*** - beschrijving (indien mogelijk de naam) van het gedetecteerde object
- ***Object*** - locatie van het object
- ***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 hierboven wordt weergegeven. Bovendien kunt u de hele lijst met gedetecteerde objecten exporteren naar een bestand (***Lijst exporteren naar een bestand***) en alle invoer over gedetecteerde objecten wissen (***Lijst leegmaken***). Als u op de knop ***Lijst vernieuwen*** klikt, wordt

de lijst met door ***Resident Shield*** gedtecteerde items vernieuwd. Als u op de knop ***Terug*** klikt, keert u terug naar de standaard ***AVG-gebruikersinterface*** (Overzicht van onderdelen).

8.13. Updatebeheer

8.13.1. Updatebeheer principes

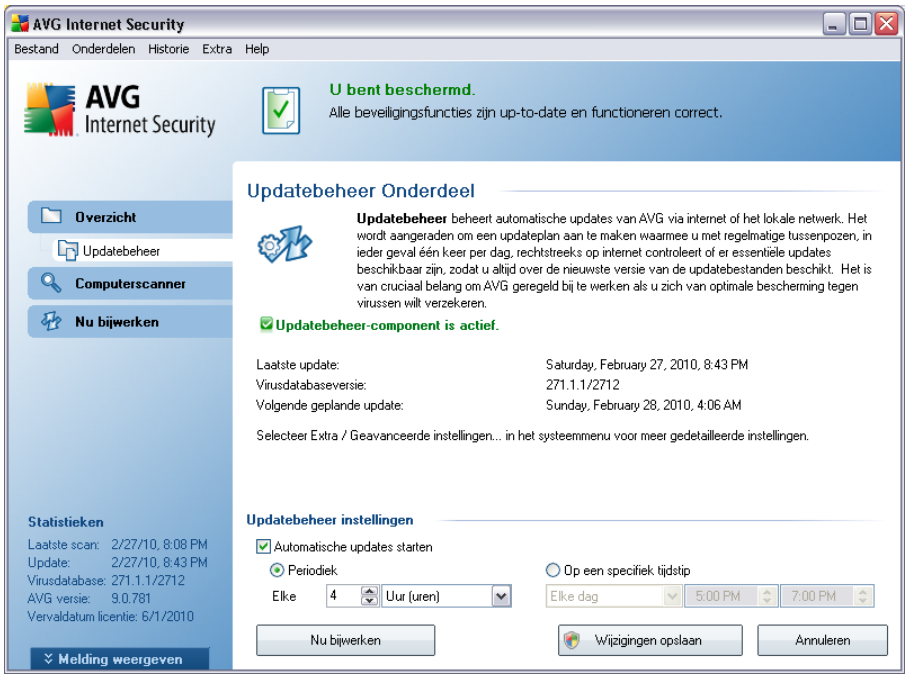
Geen enkel beveiligingsprogramma kan werkelijk garant staan voor bescherming tegen allerlei bedreigingen als het niet regelmatig wordt bijgewerkt! De makers van virussen zoeken steeds naar nieuwe tekortkomingen in software en besturingssystemen om uit te buiten. Elke dag verschijnen er nieuwe virussen, 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.

Het is cruciaal dat u regelmatig updates uitvoert voor AVG.

Het ***Updatebeheer*** helpt u bij het beheer van regelmatige updates. Met dit onderdeel kunt u automatische downloads plannen van update bestanden, van internet of via het lokale netwerk. Essentiële updates van virusdefinities dienen als dat mogelijk is, dagelijks te worden uitgevoerd. Minder urgente updates kunnen ook wekelijks worden uitgevoerd.

Opmerking: *neem het hoofdstuk AVG Updates door voor meer informatie over typen updates en updateniveaus!*

8.13.2. Updatebeheer interface



De interface van ***Updatebeheer*** biedt informatie over de functionaliteit van het onderdeel, de huidige status (*Updatebeheer is actief.*) en relevante statistische gegevens:

- ***Laatste update*** - de datum en het tijdstip waarop de database voor het laatst is bijgewerkt
- ***Virusdatabaseversie*** - het nummer van de laatste virusdatabaseversie; dit nummer wordt bij iedere nieuwe versie één hoger
- ***Volgende geplande update*** - de dag en het tijdstip waarop de volgende update van de database plaats zal vinden

Basisconfiguratie van het onderdeel

Het onderste deel van het dialoogvenster is de sectie ***Instellingen Updatebeheer*** waar u een aantal wijzigingen kunt aanbrengen in de regels die het starten van de updateprocedure bepalen. U kunt opgeven dat updatebestanden automatisch moeten worden gedownload (***Automatische updates starten***) of alleen op verzoek. Standaard is de optie ***Automatische updates starten*** ingeschakeld; het is raadzaam

die instelling aan te houden! Het regelmatig downloaden van de nieuwste updates is cruciaal voor het goed functioneren van welke vorm van beveiligingssoftware dan ook!

Bovendien bepaalt u hier wanneer de opstartprocedure moet worden gestart:

- ***Periodiek*** - geef een tijdsinterval op
- ***Op een specifiek tijdstip*** - geef datum en tijdstip op

Standaard is de optie zo ingesteld dat om de vier uur de procedure wordt gestart. We bevelen u met nadruk aan deze instelling aan te houden, tenzij u een goede reden hebt om die te wijzigen!

Opmerking: De leverancier van *heeft alle onderdelen van AVG zo ingesteld dat ze optimaal presteren. Wijzig de configuratie van AVG niet, tenzij er een goede reden is om dat wel te doen. Wijzigingen in de instellingen dienen alleen te worden uitgevoerd door ervaren gebruikers. Als u de AVG-configuratie dient te wijzigen, selecteert u in het systeemmenu de optie**Tools / Geavanceerde instellingen** en bewerkt u de AVG-configuratie in het nieuw geopende dialoogvenster AVG Geavanceerde instellingen.*

Knoppen

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

- ***Nu bijwerken*** - op verzoek wordt een onmiddellijke update uitgevoerd
- ***Wijzigingen opslaan*** - klik op deze knop om de wijzigingen die u in het dialoogvenster hebt uitgevoerd op te slaan en toe te passen
- ***Annuleren*** - klik op deze knop om het dialoogvenster te sluiten zonder wijzigingen op te slaan, en terug te keren naar de standaard ***AVG-gebruikersinterface*** (het overzicht van onderdelen)

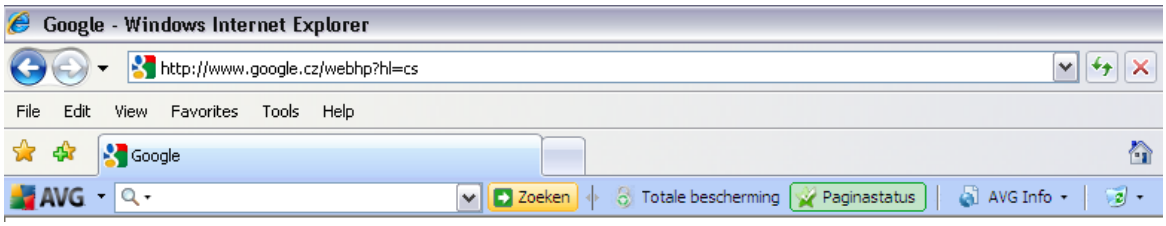
9. AVG Werkbalk Beveiliging

De AVG Werkbalk Beveiliging is een nieuw hulpprogramma dat samenwerkt met het onderdeel ***LinkScanner*** en dat de zoekresultaten van de ondersteunde internetzoekmachines (*Yahoo!, Google, Bing, Altavista en Baidu*) controleert. ***De AVG Werkbalk Beveiliging*** kan worden gebruikt om de functies van ***AVG LinkScanner*** te controleren en aan te passen.

Als u ervoor kiest om de werkbalk te installeren tijdens de installatie van **AVG 9 Internet Security**, wordt deze automatisch in uw webbrowser geïntegreerd. Als u een andere internetbrowser gebruikt (*bijvoorbeeld de Avant-browser*) kan er onverwacht gedrag optreden.

9.1. AVG Werkbalk Beveiliging Interface

De ***AVG Werkbalk Beveiliging*** is ontwikkeld voor samenwerking met ***MS Internet Explorer*** (*versie 6.0 of hoger*) en ***Mozilla Firefox*** (*versie 2.0 of hoger*). Als u eenmaal hebt besloten dat u de ***AVG Werkbalk Beveiliging*** wilt installeren (*tijdens het installatieproces van AVG is u gevraagd of u het onderdeel wel of niet wilde installeren*), het onderdeel wordt in de webbrowser meteen onder de adresbalk geplaatst:



Opmerking: *De AVG Werkbalk Beveiliging is niet bedoeld voor serverplatforms!*

Op de ***AVG Werkbalk Beveiliging*** staat het volgende:

- ***AVG-logo*** - geeft toegang tot een menu met algemene werkbalkopties. Klik op de logo-knop om naar de website van AVG (http://www.avg.com/) te gaan. Klikt u op het pijltje naast het AVG-logo, dan wordt een menu geopend met de volgende items:
    - ***Werkbalkinfo*** - een koppeling naar de introductiepagina van de ***AVG Werkbalk Beveiliging*** met aanvullende informatie over de bescherming die de werkbalk biedt
    - ***AVG 9 Internet Security starten*** - opent de interface van **AVG 9 Internet Security**

- ***Opties*** - een configuratiedialoogvenster openen waarin u de instellingen voor de ***AVG Werkbalk Beveiliging*** naar wens kunt aanpassen - zie het volgende hoofdstuk ***AVG Werkbalk Beveiliging Opties***

- ***Historie wissen*** - u kunt de *Volledige historie wissen* van de AVG Werkbalk Beveiliging, of de *Zoekgeschiedenis verwijderen, Browsergeschiedenis verwijderen, Downloadgeschiedenis verwijderen* en *Cookies verwijderen*.

- ***Update*** - controleren of er nieuwe updates beschikbaar zijn voor de ***AVG Werkbalk Beveiliging***

- ***Help*** - opties voor het openen van het Help-bestand en het verzenden van productfeedback, of details van de huidige versie van de werkbalk bekijken

- ***Zoekvak*** - typ een woord of woordgroep in het zoekvak. Druk op ***Zoeken*** om de zoekopdracht te starten met de opgegeven zoekmachine (*u kunt de gewenste zoekmachine opgeven in de Geavanceerde opties van de AVG Werkbalk Beveiliging ; u kunt kiezen uit Yahoo!, Wikipedia, Baidu, WebHledani of Yandex*). Het maakt niet uit welke pagina er op dat moment wordt weergegeven. Aan het zoekvak is bovendien een keuzelijst gekoppeld met eerdere zoekopdrachten. De resultaten van zoekopdrachten die u via dit zoekvak opgeeft, worden geanalyseerd met ***AVG Search-Shield***.

- ***Totale bescherming*** - deze knop wordt optioneel weergegeven als ***Totale bescherming***/ ***Beperkte bescherming*** / ***Geen bescherming***, afhankelijk van de configuratie van **AVG 9 Internet Security**

- ***Paginastatus*** - deze knop in de werkbalk geeft evaluatie-informatie over de webpagina die op dat moment wordt weergegeven, gebaseerd op de instellingen van het onderdeel ***AVG Search-Shield*** (*pagina is veilig / verdacht / zonder meer gevaarlijk / bevat bedreigingen / kon niet worden gescand*). Klik op de knop om een informatievenster te openen dat gedetailleerde gegevens bevat over de specifieke webpagina.

- ***AVG Info*** - bevat koppelingen naar belangrijke informatie over beveiliging op de website van AVG (http://www.avg.com/).

  - ***Werkbalkinfo*** - een koppeling naar de introductiepagina van de ***AVG Werkbalk Beveiliging*** met aanvullende informatie over de bescherming die de werkbalk biedt

  - ***Over bedreigingen*** - opent de webpagina van AVG met informatie over

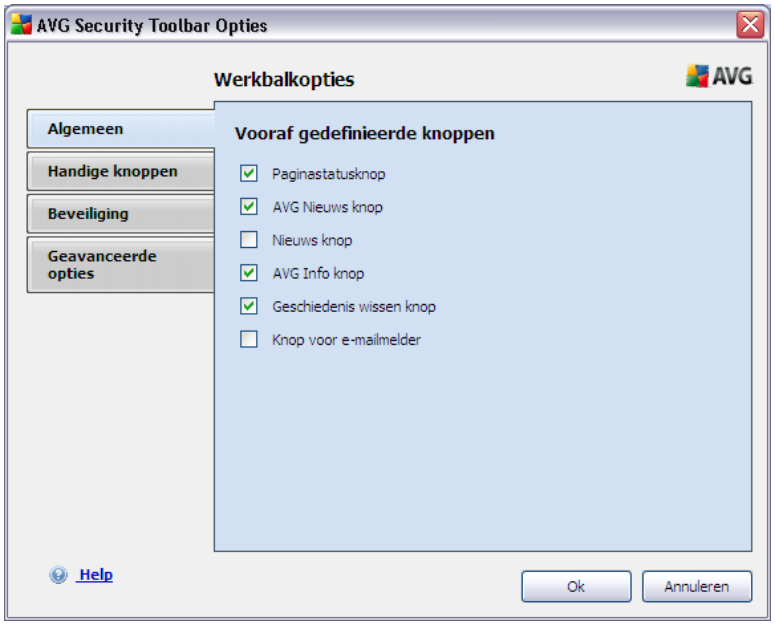
recente virussen en internetbedreigingen

- ***AVG-nieuws*** - opent de webpagina met het meest recente persbericht over AVG
- ***Huidig bedreigingsniveau*** - opent de webpagina van het viruslab met een grafische weergave van het huidige bedreigingsniveau op internet
- ***Virusencyclopedie*** - opent de pagina Virusencyclopedie waarop u naar gedetailleerde informatie kunt zoeken op naam van virussen

9.2. AVG Werkbalk Beveiliging

Alle parameters die u kunt configureren voor de ***AVG Werkbalk Beveiliging*** zijn direct toegankelijk in het venster van de ***AVG Werkbalk Beveiliging***. U opent de interface met het menu-item *AVG / Opties* van de werkbalk in een nieuw dialoogvenster ***Werkbalkopties*** dat verdeeld is in vier secties:

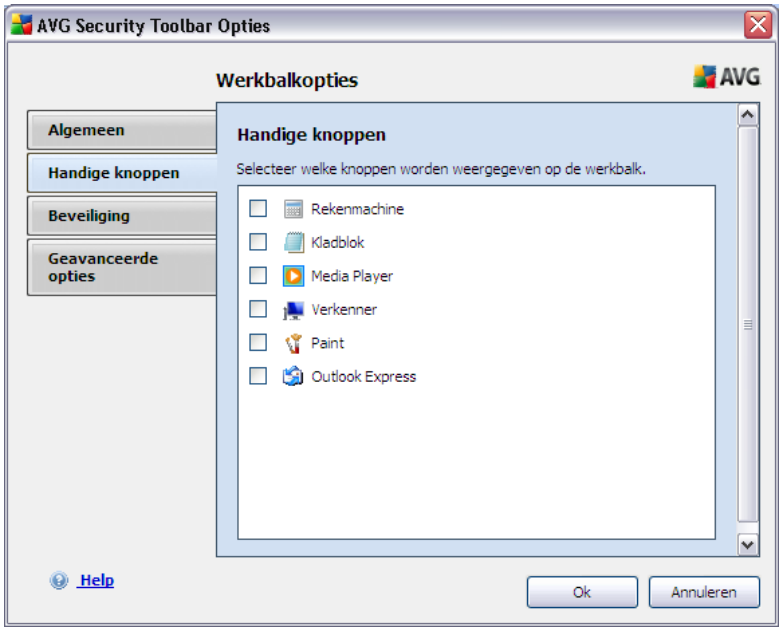
9.2.1. Tabblad Algemeen



Op dit tabblad kunt u opgeven welke knoppen voor de besturing van de werkbalk moeten worden weergegeven of verborgen in het venster van de ***AVG Werkbalk Beveiliging***. Schakel de selectievakjes in voor de knoppen die u wilt weergeven. Hieronder vindt u een beschrijving van de functie van de knoppen:

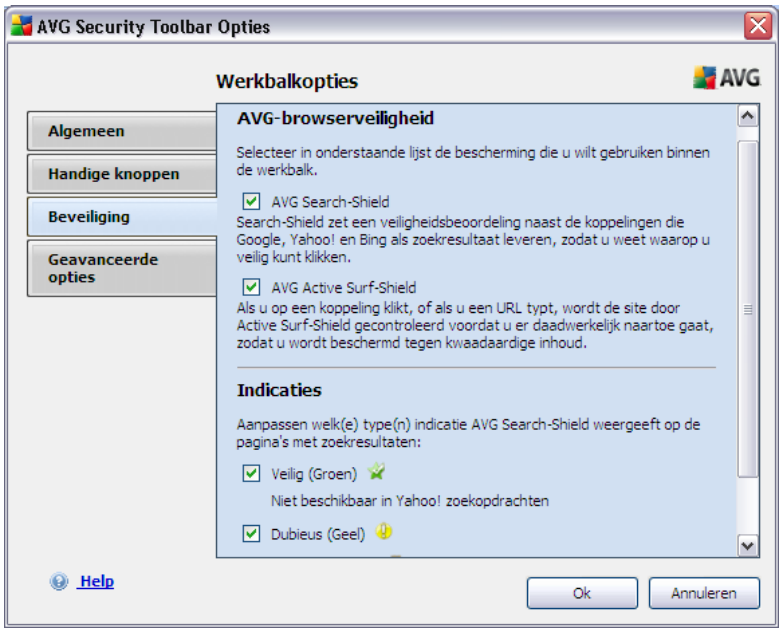
- ***AVG Nieuws knop*** - met deze knop opent u een webpagina met het meest recente persbericht over AVG
- ***Nieuws knop*** - met deze knop krijgt u toegang tot een gestructureerd overzicht van het dagelijkse nieuws
- ***AVG Info knop*** - via deze knop krijgt u informatie over de AVG Werkbalk, over actuele bedreigingen en het bedreigingsniveau op internet en kunt u de virusencyclopedie openen en nieuws over AVG-producten opvragen
- ***Knop Historie wissen*** - met deze knop kunt u devolledige historie wissen, of de Zoekgeschiedenis verwijderen, Browsergeschiedenis verwijderen, Downloadgeschiedenis verwijderen, ofCookies verwijderen, direct vanuit het venster van de AVG Werkbalk Beveiliging.

9.2.2. Tabblad Handige knoppen



U gebruikt het tabblad ***Handige knoppen*** om toepassingen uit een lijst te selecteren en hun pictogram in de werkbalk weer te geven. U kunt deze pictogrammen vervolgens gebruiken als een snelkoppeling om de desbetreffende toepassing meteen te starten.

9.2.3. Tabblad Beveiliging

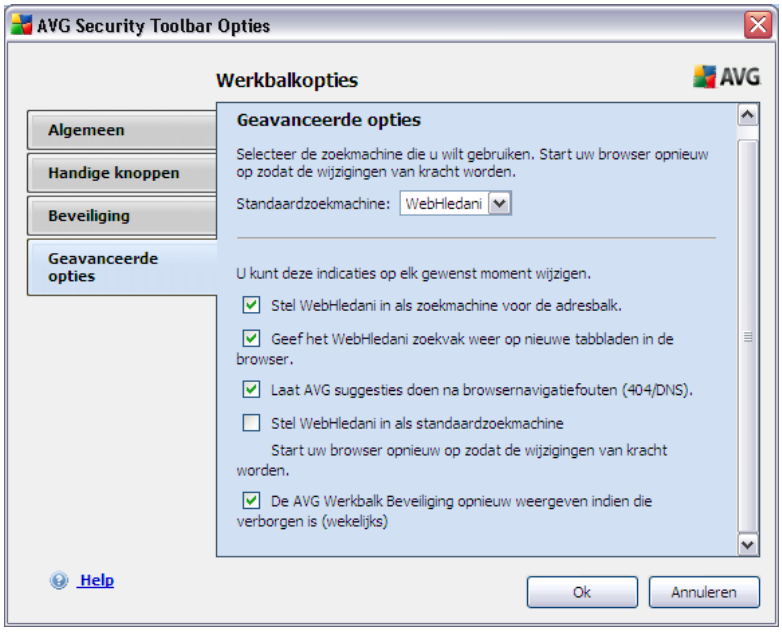


Het tabblad ***Beveiliging***is verdeeld in twee secties, ***AVG-browserveiligheid*** en ***Indicaties***, waar u met behulp van selectievakjes kunt aangeven welke functionaliteit van de ***AVG Werkbalk Beveiliging*** u wilt gebruiken:

- ***AVG-browserveiligheid*** - schakel met deze optie de services ***AVG Search-Shield*** en/of ***AVG Active Surf-Shield*** in of uit
- ***Indicaties*** - selecteer de pictogrammen die moeten worden gebruikt om indicaties aan te geven bij zoekresultaten van het onderdeel ***AVG Search-Shield***:
    - pagina is veilig
    - pagina is enigszins verdacht
    - er staan koppelingen op de pagina naar gevaarlijke pagina's
    - er staan actieve bedreigingen op de pagina
    - De pagina is niet toegankelijk en is daarom niet gescand

Schakel het selectievakje in bij een optie als u over die specifieke vorm van bedreiging wilt worden geïnformeerd. U kunt echter de weergave van de rode indicatie die is toegewezen aan pagina's met actieve en gevaarlijke bedreigingen, niet uitschakelen. ***We raden u opnieuw aan om de standaardconfiguratie, ingesteld door de leverancier van het programma, aan te houden, tenzij u een goede reden hebt om daarvan af te wijken.***

9.2.4. Tabblad Geavanceerde opties



Op het tabblad ***Geavanceerde opties*** selecteert u eerste de zoekmachine die u standaard wilt gebruiken. U kunt kiezen uit *Yahoo!, Baidu, WebHledani* en *Yandex*. Nadat u de standaardzoekmachine hebt gewijzigd, start u uw internetbrowser opnieuw op om de wijziging door te voeren.

U kunt ook bepaalde instellingen voor de ***AVG Werkbalk Beveiliging*** activeren of uitschakelen:

- ***Stel Yahoo! in als zoekmachine voor de adresbalk*** - (*standaard ingeschakeld*) - als het selectievakje bij deze optie is ingeschakeld, kunt u een trefwoord voor een zoekopdracht direct in het tekstvak op de adresbalk van uw internetbrowser typen om de zoekmachine van Yahoo! opdracht te geven naar bijbehorende websites te zoeken.

- ***Laat AVG suggesties doen na browsernavigatiefouten (404/DNS)*** - (

standaard ingeschakeld) - als u tijdens het zoeken op een niet-bestaande pagina terechtkomt, of op een pagina die niet kan worden weer gegeven (404-fout), wordt er automatisch een webpagina weergegeven met daarop een overzicht van alternatieve pagina's die met het onderwerp verwant zijn en waaruit u kunt kiezen.

- ***Stel Yahoo! in als zoekprovider voor uw browser*** - (*standaard uitgeschakeld*) - Yahoo! is de standaard zoekmachine voor een zoekopdracht op internet vanuit de AVG Werkbalk Beveiliging; als u deze optie inschakelt, wordt Yahoo! ook de standaard zoekmachine in uw browser.

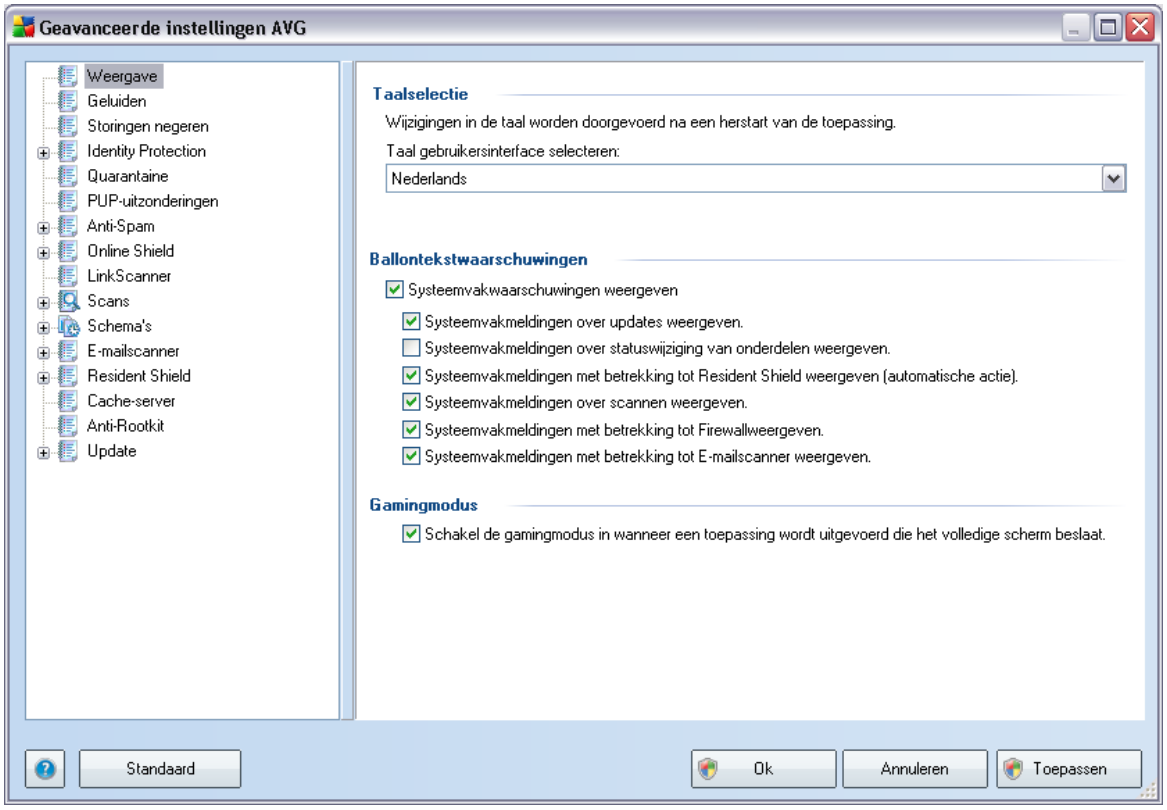
- ***De AVG Werkbalk Beveiliging opnieuw weergeven indien die verborgen is (wekelijks)*** - (*standaard ingeschakeld*) - deze optie is standaard ingeschakeld en zorgt ervoor dat wanneer de ***AVG Werkbalk Beveiliging*** per ongeluk wordt verborgen, hij in ieder geval na verloop van een week weer zal worden weergegeven.

10. AVG Geavanceerde instellingen

Het dialoogvenster voor een geavanceerde configuratie van **AVG 9 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 rechter deelvenster te openen.

10.1. Weergave

De eerste optie in de navigatiestructuur, ***Weergave***, verwijst naar de algemene instellingen voor de AVG gebruikersinterface en een paar basisinstellingen voor de manier waarop de toepassing werkt:



Taalselectie

In de sectie ***Taalselectie*** kunt u in de vervolgkeuzelijst een taal selecteren; die taal wordt dan overal in de AVG Gebruikersinterface toegepast. In het vervolgkeuzemenu staan alleen de talen die u tijdens de installatieprocedurehebt geselecteerd (zie hoofdstuk Aangepaste installatie - Onderdelen selecteren). Voor het voltooien van de procedure om over te stappen op een andere taal, zult u de gebruikersinterface opnieuw moeten starten; ga als volgt te werk:

- Selecteer de gewenste taal voor de toepassing en bevestig uw selectie door op de knop ***Toepassen*** te klikken (in de rechterbenedenhoek)
- Klik op de knop ***OK*** om te bevestigen
- Er wordt een nieuw dialoogvenster geopend met de mededeling dat een wijziging van de taal voor de AVG-gebruikersinterface vereist dat de toepassing opnieuw wordt opgestart

Ballontekstwaarschuwingen

In dit gedeelte kunt u de weergave van ballontekstwaarschuwingen over de status van de toepassing in- en uitschakelen. Standaard worden de ballontekstwaarschuwingen weergegeven en het is raadzaam die instelling aan te houden! De ballontekstwaarschuwingen geven informatie wanneer er iets in de status van een onderdeel verandert en verdienen daarom aandacht!

Als u echter om de een of andere reden de weergave van ballontekstwaarschuwingen wilt onderdrukken, of als u alleen bepaalde ballontekstwaarschuwingen wilt weergeven (van bijvoorbeeld een bepaald AVG onderdeel), kunt u uw voorkeuren opgeven door de volgende opties in- of uit te schakelen:

- ***Systeemvakmeldingen weergeven*** - standaard staat een vinkje bij deze optie (*ingeschakeld*) en worden Systeemvakmeldingen weergegeven. Schakel dit selectievakje uit als u in het geheel geen gebruik wilt maken van Systeemvakmeldingen. Als u de optie inschakelt, kunt u nader bepalen welke meldingen u wilt weergeven:

- ***Systeemvakmeldingen over updates*** weergeven - maak een keuze of u meldingen van het starten, de voortgang en het voltooien van de AVG update wilt weergeven;

- ***Systeemvakmeldingen over statuswijziging van onderdelen weergeven*** - maak een keuze of u informatie over de activiteit/ inactiviteit van een onderdeel of mogelijk daarmee samenhangende problemen wilt weergeven. Bij het rapporteren van de foutstatus van een onderdeel, heeft deze optie hetzelfde effect als de informatieve functie van het systeemvakpictogram (kleurwijzigingen) dat een probleem aangeeft met een AVG onderdeel;

- ***Systeemvakmeldingen met betrekking tot Resident Shield weergeven*** - maak een keuze of u meldingen bij procedures voor het opslaan, kopiëren en openen van bestanden wilt weergeven of niet (*deze configuratie wordt alleen weergegeven als de optie Automatisch herstel in Resident Shield is geactiveerd*);

- ***Systeemvakmeldingen over scannen*** weergeven - maak een keuze of u meldingen van het automatisch starten van geplande scans, de voortgang en de resultaten wilt weergeven;

- ***Systeemvakmeldingen met betrekking tot Firewall weergeven*** - maak een keuze of informatie over de status van Firewall en verwante processen, bijv. waarschuwingen over het inschakelen/uitschakelen van het onderdeel, meldingen van geblokkeerd verkeer, enz., moet worden weergegeven;

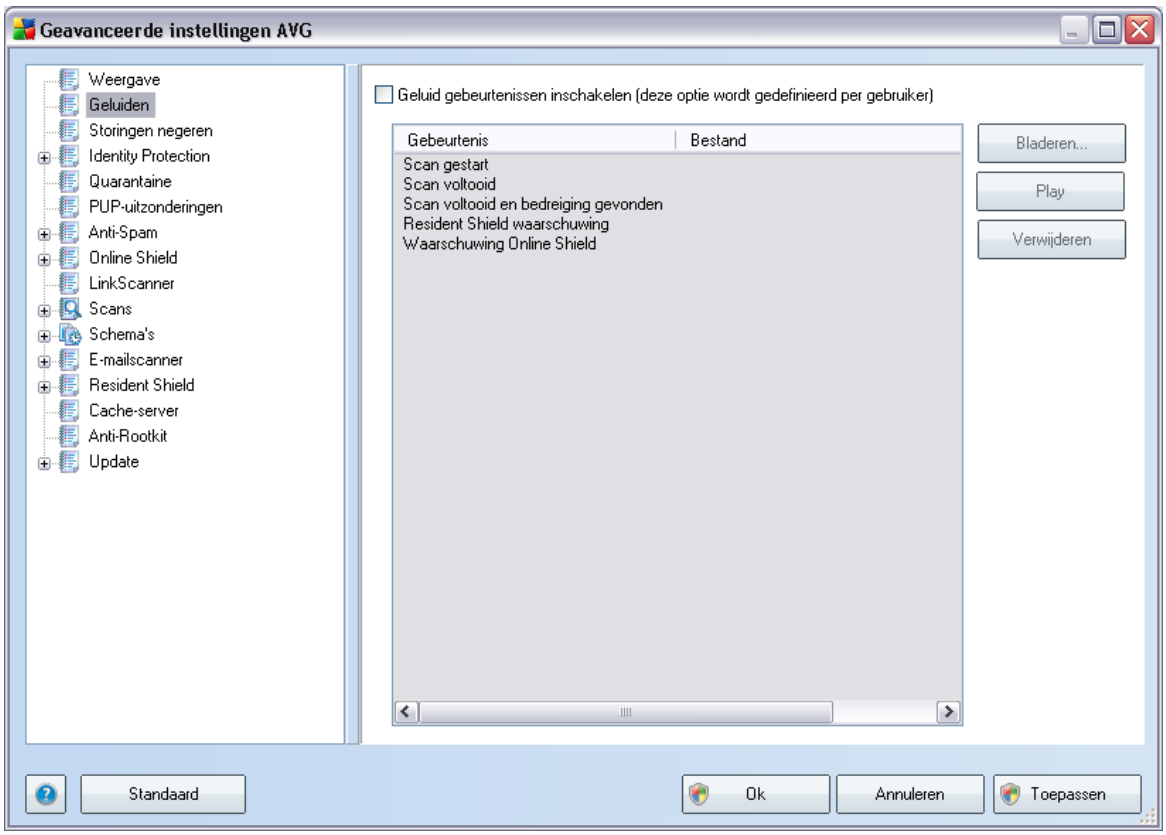
- ***Systeemvakwaarschuwingen die betrekking hebben op de e-mailscanner weergeven*** - maak een keuze of informatie over het scannen van alle binnenkomende en uitgaande e-mailberichten moet worden weergegeven.

Gamingmodus

Deze AVG-functie is ontworpen voor schermvullende toepassingen, waarbij AVG-ballonteksten (*die bijvoorbeeld worden weergegeven wanneer er een geplande scan start*) een verstorend effect zouden kunnen hebben (*de toepassing zou geminimaliseerd kunnen worden of de afbeeldingen zouden beschadigd kunnen worden*). Om dat te voorkomen houdt u het selectievakje ***Schakel de gamingmodus in wanneer een toepassing wordt uitgevoerd die het volledige scherm beslaat*** ingeschakeld (*standaard ingeschakeld*).

10.2. Geluiden

In het dialoogvenster ***Geluiden*** kunt u opgeven of u op bepaalde AVG-acties opmerkzaam gemaakt wilt worden met een geluidssignaal. Schakel, als u dat wilt, het selectievakje in bij ***Geluid gebeurtenissen inschakelen*** (*standaard uitgeschakeld*) om de lijst met AVG-acties te activeren:

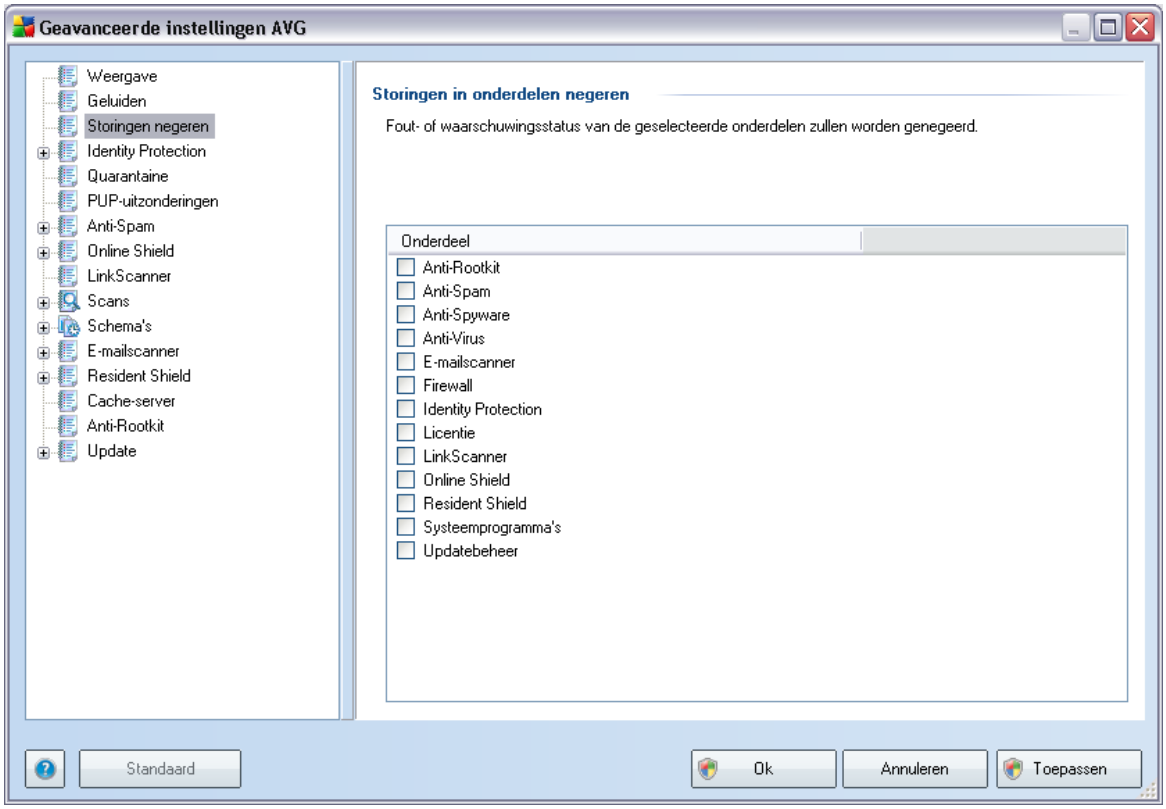


Selecteer dan een gebeurtenis in de lijst en zoek (***Bladeren***) op de vaste schijf een geluid dat u aan de gebeurtenis wilt toewijzen. Als u een voorbeeld van het geluid wilt afspelen, selecteert u de gebeurtenis in de lijst en klikt u op de knop ***Afspelen***. Klik op de knop ***Verwijderen*** als u de koppeling tussen een gebeurtenis en een geluidssignaal wilt verbreken.

Opmerking: *alleen *.wav-geluiden worden ondersteund*

10.3. Storingen negeren

In het dialoogvenster ***Storingen in onderdelen negeren*** kunt u de onderdelen inschakelen waarover u geen informatie wilt ontvangen:



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

- ***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,
- tekstbeschrijving van het huidige probleem in het gedeelte ***Info Beveiligingsstatus*** van het hoofdvenster van AVG.

Er zou zich een situatie kunnen voordoen waarin u een onderdeel tijdelijk moet uitschakelen (*. Dit wordt niet aanbevolen. U zou moeten proberen alle onderdelen permanent ingeschakeld en in de standaardconfiguratie te houden, maar toch kan een*

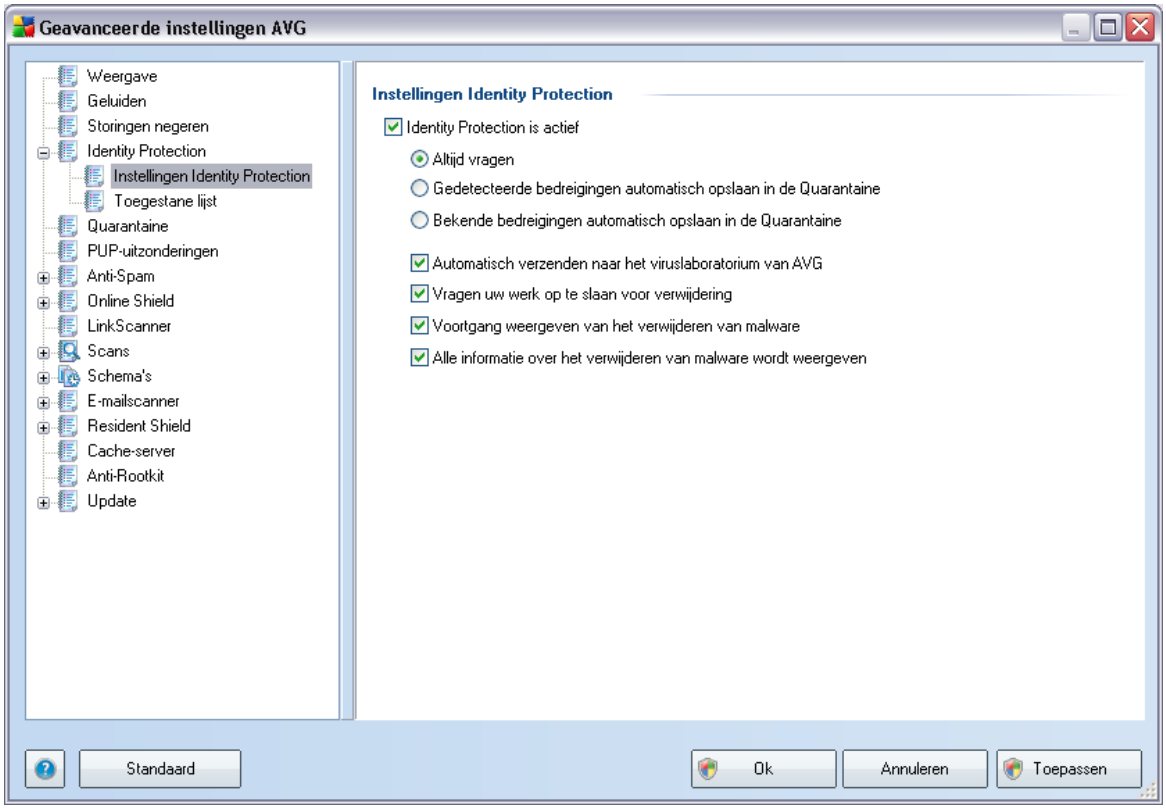
dergelijke situatie zich voordoen). In dat geval rapporteert het systeemvakpictogram automatisch de foutstatus van het onderdeel. In dit specifieke geval kan echter niet worden gesproken van een echte fout, omdat u deze opzettelijk hebt veroorzaakt en omdat u zich bewust bent van het potentiële risico. 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 hierboven onderdelen selecteren die een foutstatus hebben (*of die uitgeschakeld zijn*) en waarover u niet wilt worden geïnformeerd. Voor specifieke onderdelen is dezelfde optie ***Storingen in onderdelen negeren*** ook beschikbaar rechtstreeks vanuit het overzicht met onderdelen in het hoofdvenster van AVG.

10.4. Identity Protection

10.4.1. Identity Protection instellingen

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



Identity Protection is actief (*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*** (*standaard ingeschakeld*) - bij detectie van een bedreiging wordt u gevraagd of deze naar de Quarantaine moet worden verplaatst, zodat u zeker weet dat er geen toepassingen naar de 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 de ***AVG Quarantaine***. Bij de standaardinstelling zal u bij detectie van een bedreiging worden gevraagd of die naar de Quarantaine moet worden verplaatst, zodat u zeker weet dat er geen toepassingen naar de Quarantaine worden verplaatst die u wilt uitvoeren.

- ***Bekende bedreigingen automatisch opslaan in de Quarantaine*** - dit selectievakje moet ingeschakeld blijven als u wilt dat alle toepassingen die worden gedetecteerd als mogelijke malware automatisch en meteen naar de ***AVG Quarantaine*** worden verplaatst.

U kunt ook specifieke opties toewijzen als u meer functies van ***Identity Protection*** wilt activeren:

- ***Automatisch verzenden naar AVG Viruslabs*** - (*standaard ingeschakeld*): als u dit selectievakje niet uitschakelt, helpt u mee de database met informatie over schadelijke activiteiten op internet bij te houden die ons assisteert bij het detecteren van nieuwe bedreigingen.

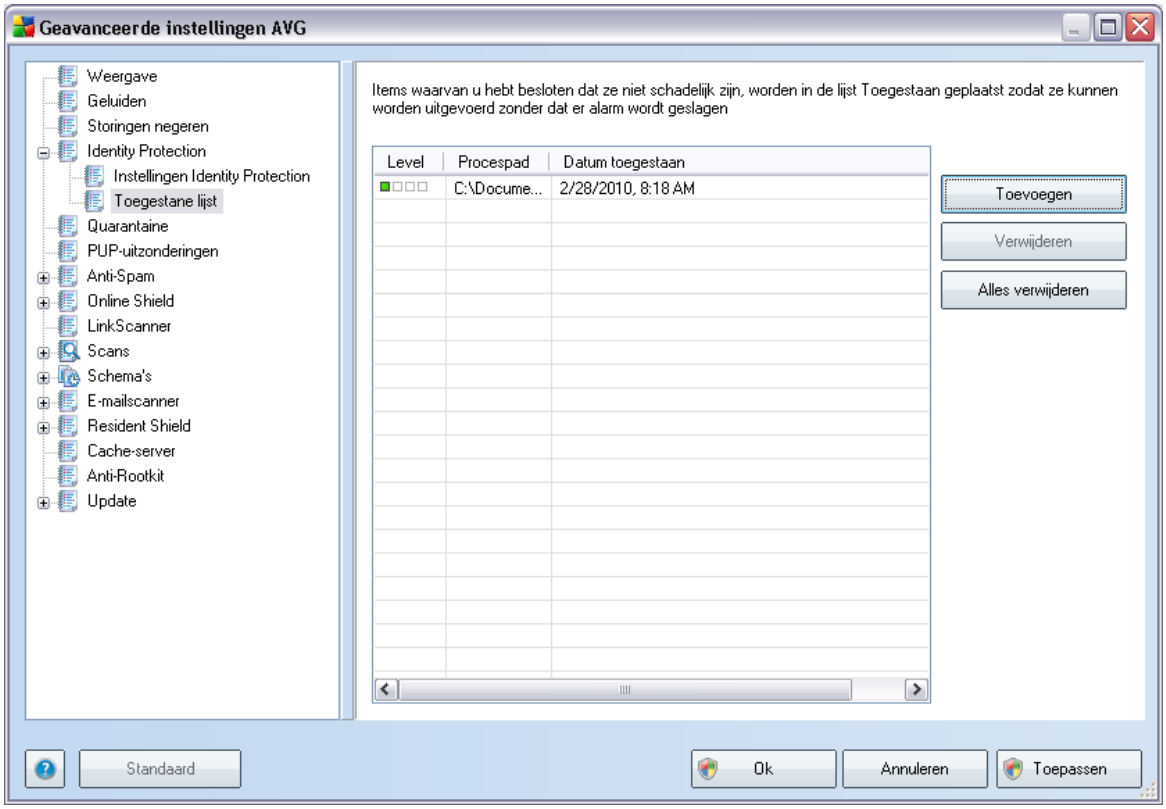
- ***Vragen uw werk op te slaan voor verwijdering***- (*standaard ingeschakeld*) - dit selectievakje moet ingeschakeld blijven als u wilt worden gewaarschuwd voordat toepassingen die worden herkend als mogelijke malware, worden verplaatst naar de Quarantaine. Als detectie plaatsvindt terwijl u met de toepassing aan het werk bent, zou namelijk een project verloren kunnen gaan als u dat niet eerst opsloeg. Standaard is de optie ingeschakeld en we adviseren nadrukkelijk om deze niet uit te schakelen.

- ***Voortgang weergeven van het verwijderen van malware***- (*standaard ingeschakeld*) - als deze optie is ingeschakeld, zal bij verwijdering van gedetecteerde malware een nieuw dialoogvenster worden geopend waarin de voortgang van het verplaatsen van de malware naar de Quarantaine wordt weergegeven.

- ***Alle informatie over het verwijderen van malware weergeven*** - (*standaard ingeschakeld*) - als deze optie is ingeschakeld, geeft Identity Protection gedetailleerde informatie weer over elk object dat naar de Quarantaine wordt verplaatst (*de ernst van de bedreiging, de plaats waar de bedreiging is geïnstalleerd, enz.*).

10.4.2. Lijst Toegestaan

Als u in het dialoogvenster ***Instellingen voor Identity Protection*** het selectievakje bij de optie ***Gedetecteerde bedreigingen automatisch opslaan in de Quarantaine*** niet hebt ingeschakeld, wordt u iedere keer dat er mogelijk gevaarlijke malware wordt gedetecteerd, gevraagd of die moet worden verwijderd. Als u op dat moment aangeeft dat de verdachte toepassing (*verdacht op grond van het gedrag van de toepassing*) veilig is, en u bevestigt dat u de toepassing wilt handhaven op uw computer, wordt de toepassing toegevoegd aan de zogenaamde lijst ***Toegestaan***, en zal hij niet opnieuw worden gerapporteerd als mogelijk gevaarlijk:



In de lijst ***Toegestaan*** staat de volgende informatie over elke toepassing:

- ***Niveau*** - grafische aanduiding voor het bedreigingsniveau van het proces op een schaal van vrij onbelangrijk (■□□□) tot kritiek (■■■■)
- ***Procespad*** - pad naar het uitvoerbare bestand van de toepassing (*het proces van de toepassing*)

- ***Datum toegestaan*** - datum waarop u de toepassing handmatig als veilig hebt beoordeeld

Knoppen

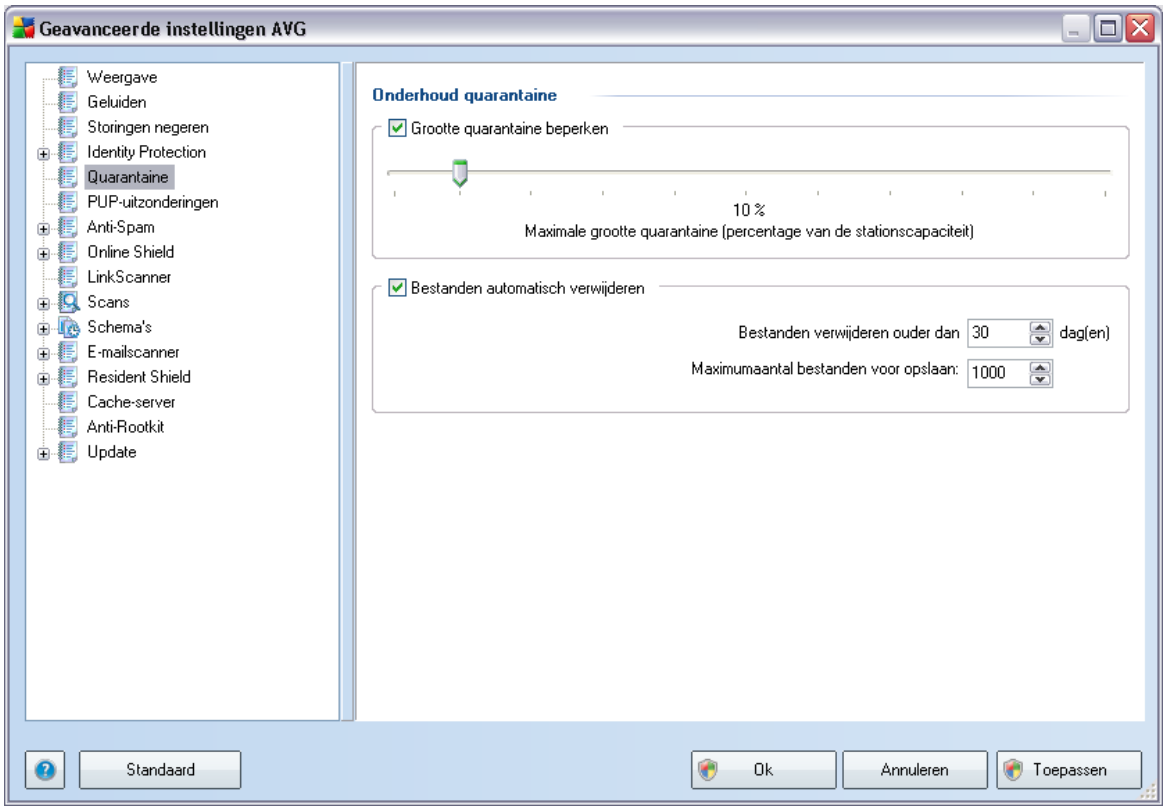
Het dialoogvenster met de lijst ***Toegestaan*** heeft de volgende knoppen:

- ***Toevoegen*** - klik op deze knop om een nieuwe toepassing aan de lijst Toegestaan toe te voegen. Het volgende dialoogvenster wordt dan geopend:

  - ***Bestand*** - Typ het volledige pad naar het bestand (*de toepassing*) die u als uitzondering wilt markeren
  - ***Checksum*** - de unieke "handtekening" van het gekozen bestand. Deze handtekening bestaat uit een automatisch gegenereerde tekenreeks op basis waarvan AVG het gekozen bestand onmiskenbaar van andere bestanden kan onderscheiden. Deze handtekening wordt gegenereerd en weergegeven nadat het bestand is toegevoegd.
  - ***Elke locatie*** - gebruik geen volledige locatie - als u dit bestand alleen op deze specifieke locatie als uitzondering wilt definiëren, schakelt u dit selectievakje niet in

- ***Verwijderen*** - klik op deze knop om de geselecteerde toepassing uit de lijst te verwijderen
- ***Alles verwijderen*** - klik op deze knop om alle toepassingen te verwijderen

10.5. Quarantaine



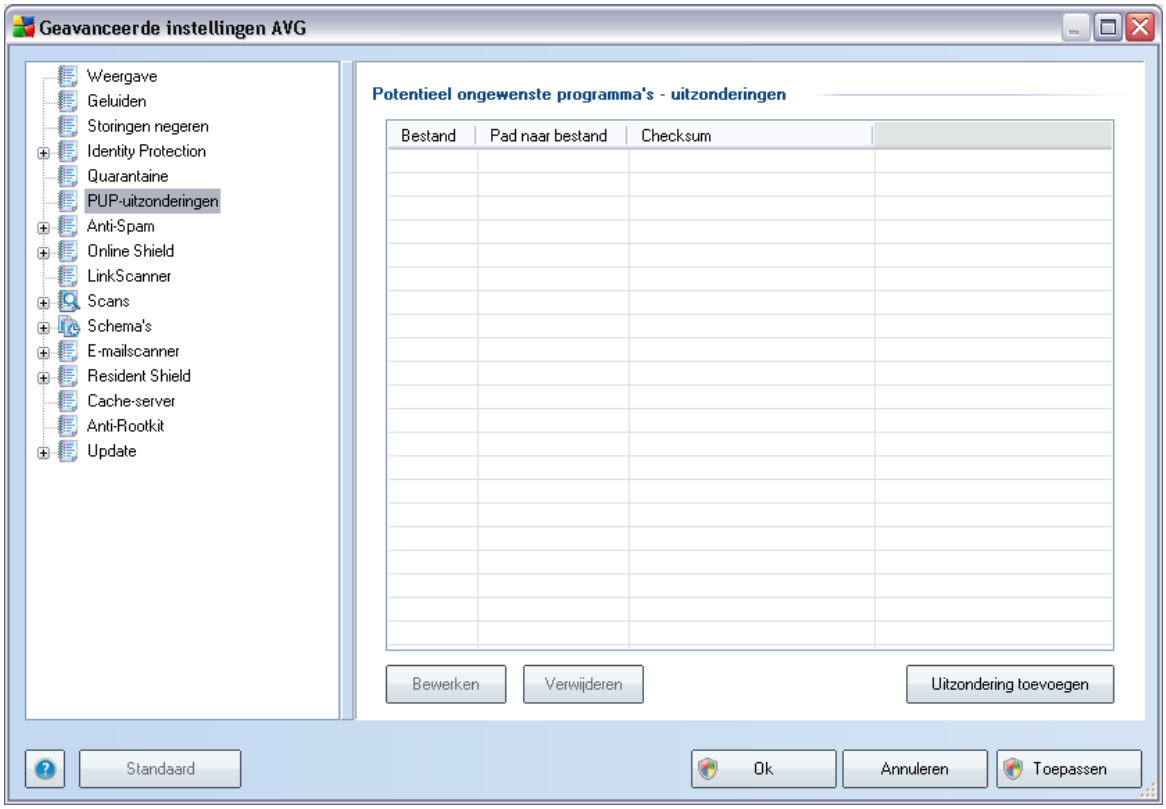
In het dialoogvenster ***Onderhoud quarantaine*** kunt u verschillende parameters instellen voor het beheer van objecten die zijn opgeslagen in ***Quarantaine***:

- ***Grootte Quarantaine beperken*** - geef met behulp van de schuifbalk een maximale grootte op voor ***Quarantaine***. U geeft de grootte op in verhouding met 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***)

10.6. PUP-uitzonderingen

AVG 9 Internet Security is in staat om uitvoerbare toepassingen en DLL-bibliotheken te analyseren en detecteren die binnen het systeem mogelijk ongewenst zijn. De gebruiker zal in sommige gevallen bepaalde gedetecteerde ongewenste programma's willen behouden (*programma's die de gebruiker opzettelijk heeft geïnstalleerd*). Sommige programma's bevatten adware. Dat is vooral het geval bij gratis programma's. Dergelijke adware wordt door AVG mogelijk gedetecteerd en gerapporteerd als een ***Potentieel ongewenst programma (PUP)***. Als u een dergelijk programma niet van uw computer wilt verwijderen, kunt u het desbetreffende programma definiëren als een uitzondering:

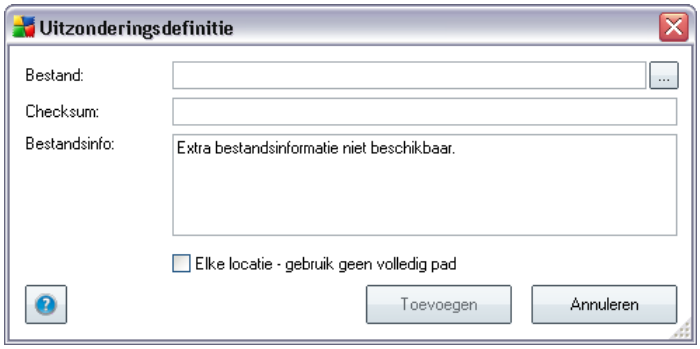


In het dialoogvenster ***Uitzonderingen voor mogelijk ongewenste programma's*** staat een lijst met eerder als zodanig gedefinieerde en geldige uitzonderingen op mogelijk ongewenste programma's. U kunt de lijst bewerken, bestaande items verwijderen en nieuwe uitzonderingen toevoegen. De volgende informatie wordt in de lijst weergegeven voor elke uitzondering:

- ***Bestand*** - de naam van de desbetreffende toepassing
- ***Pad naar bestand*** - het volledige pad naar het bestand
- ***Checksum*** - de unieke "handtekening" van het gekozen bestand. Deze handtekening bestaat uit een automatisch gegenereerde tekenreeks op basis waarvan AVG het gekozen bestand onmiskenbaar van andere bestanden kan onderscheiden. Deze handtekening wordt gegenereerd en weergegeven nadat het bestand is toegevoegd.

Knoppen

- ***Bewerken*** - er wordt een nieuw dialoogvenster geopend (*identiek met het dialoogvenster voor het toevoegen van een nieuwe uitzondering, zie hieronder*) voor het bewerken van een eerder gedefinieerde uitzondering, waarin u parameters kunt wijzigen
- ***Verwijderen*** - het geselecteerde item wordt verwijderd uit de lijst met uitzonderingen
- ***Uitzondering toevoegen*** - er wordt een dialoogvenster geopend voor het bewerken van de parameters van een nieuw toe te voegen uitzondering:

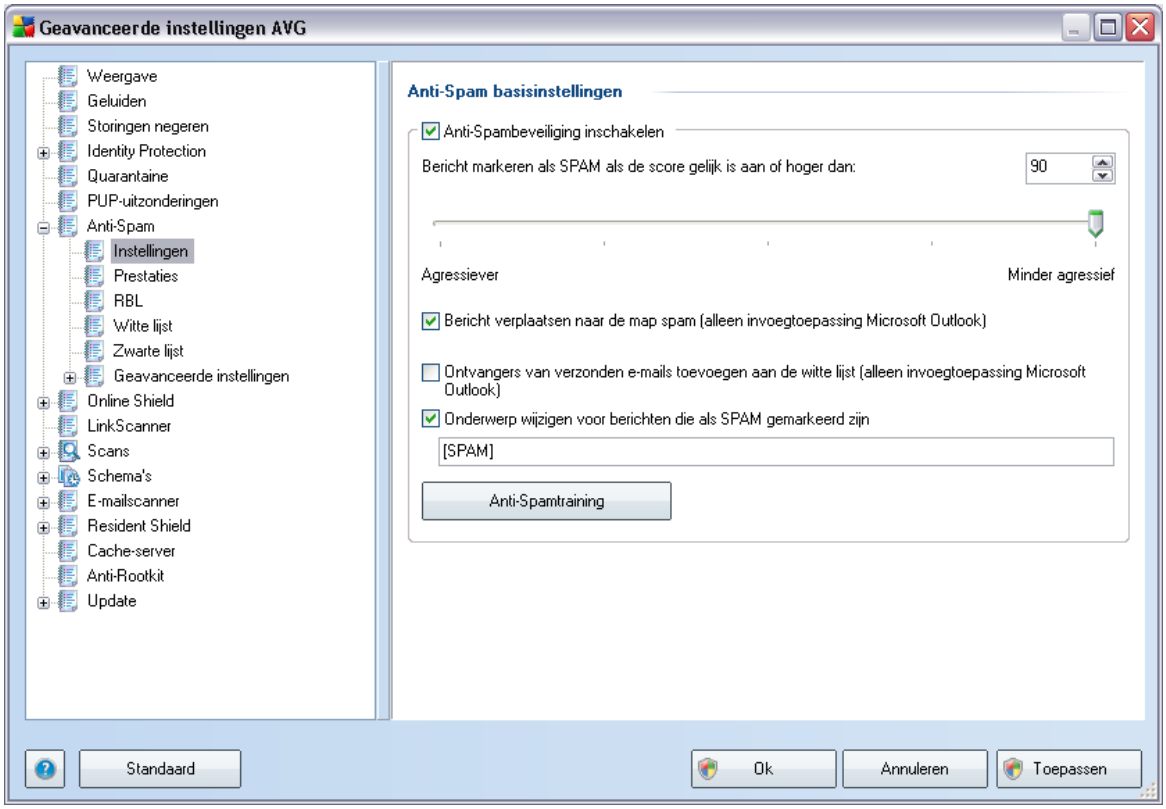


  - ***Bestand*** - Typ het volledige pad naar het bestand dat u wilt markeren als een uitzondering
  - ***Checksum*** - de unieke "handtekening" van het gekozen bestand. Deze handtekening bestaat uit een automatisch gegenereerde tekenreeks op basis waarvan AVG het gekozen bestand onmiskenbaar van andere bestanden kan onderscheiden. Deze handtekening wordt gegenereerd en weergegeven nadat het bestand is toegevoegd.

- ***Bestands info*** - alle aanvullende informatie die voor het bestand beschikbaar is (*licentie-/versie-informatie, enz.*)
- ***Elke locatie - gebruik geen volledige locatie*** - als u dit bestand alleen op deze specifieke locatie als uitzondering wilt definiëren, schakelt u dit selectievakje niet in

10.7. Anti-Spam

10.7.1. Instellingen



In het dialoogvenster***Basisinstellingen voor Anti-Spam*** kunt u het selectievakje ***Anti-Spambeveiliging 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 aanbevolen dat alleen te veranderen 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 instelling ***Bericht als spam markeren als score hoger is dan*** aanpassen door een waarde tussen *0 en 100* in te voeren, of door de schuifbalk naar links of rechts te slepen (*als u de schuifbalk gebruikt, is het bereik beperkt tot 50-90*).

Over het algemeen is het raadzaam de drempel in te stellen op een waarde tussen 50 en 90, of op 90 als u niet zeker weet wat u moet doen. Hieronder volgt een algemeen overzicht van de scoredrempel.

- ***Waarde 90-99*** - De meeste binnenkomende e-mailberichten worden normaal afgeleverd (zonder als spam gemarkeerd te worden). De gemakkelijkst herkenbare spam wordt gefilterd, maar een aanzienlijke hoeveelheid spam wordt nog doorgelaten.
- ***Waarde 80-89*** - E-mailberichten waarvan de kans groot is dat ze spam bevatten, worden gefilterd. Het kan zijn dat sommige niet-spamberichten ook gefilterd worden.
- ***Waarde 60-79*** - Een vrij agressieve configuratie. E-mailberichten die waarschijnlijk spam zijn, worden gefilterd. Niet-spamberichten worden waarschijnlijk ook als spam aangeduid.
- ***Waarde 1-59*** - Een zeer agressieve configuratie. Zowel niet-spamberichten als echte spamberichten worden gefilterd. Deze instelling is niet raadzaam voor normaal gebruik.
- ***Waarde 0*** - In deze modus ontvangt u alleen e-mailberichten van afzenders op uw ***witte lijst***. Alle andere e-mailberichten worden als spam beschouwd. ***Deze instelling is niet raadzaam voor normaal gebruik.***

In het dialoogvenster ***Basisinstellingen voor Anti-Spam*** kunt u verder opgeven wat er met gedetecteerde spamberichten moet gebeuren:

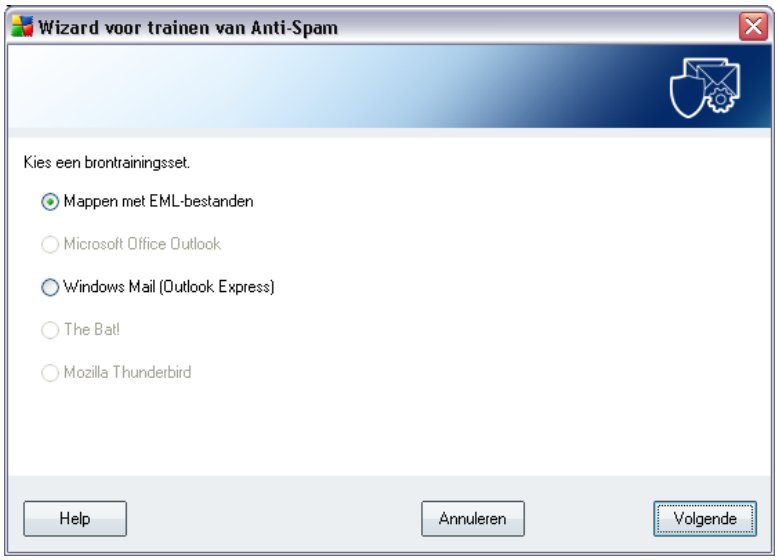
- ***Bericht verplaatsen naar de map spam*** - schakel dit selectievakje in als elk bericht met spam dat is gedetecteerd, automatisch naar de daarvoor aangewezen map van uw e-mailclient moet worden verplaatst;
- ***Ontvangers van verzonden e-mails toevoegen aan de witte lijst***- schakel dit selectievakje in om aan te geven dat alle ontvangers van verzonden e-mails kunnen worden vertrouwd, en dat e-mail die vanaf hun e-mailadressen worden 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 op de onderwerpsregel van het bericht; U kunt het desbetreffende woord of teken in het geactiveerde tekstveld typen.

Knoppen

Anti-Spam trainen - klik op deze knop om de ***wizard Anti-Spamtraining*** te starten die gedetailleerd wordt beschreven in het volgende hoofdstuk.

In het eerste dialoogvenster van de ***wizard Anti-Spamtraining*** wordt u gevraagd de bron van e-mailberichten te selecteren die u voor training wilt gebruiken. Over het algemeen gebruikt u daarvoor de e-mails die onterecht zijn aangemerkt als SPAM en spamberichten die niet als zodanig zijn herkend.



U kunt kiezen uit de volgende opties:

- ***Een specifieke e-mailclient*** - als u met één van de genoemde e-mailclients (*MS Outlook, Outlook Express, The Bat!, Mozilla Thunderbird*) werkt, kiest u de corresponderende optie
- ***Map met EML-bestanden*** - als u een ander e-mailprogramma gebruikt, dient u eerst de berichten in een bepaalde map op te slaan (*in .eml format*), of

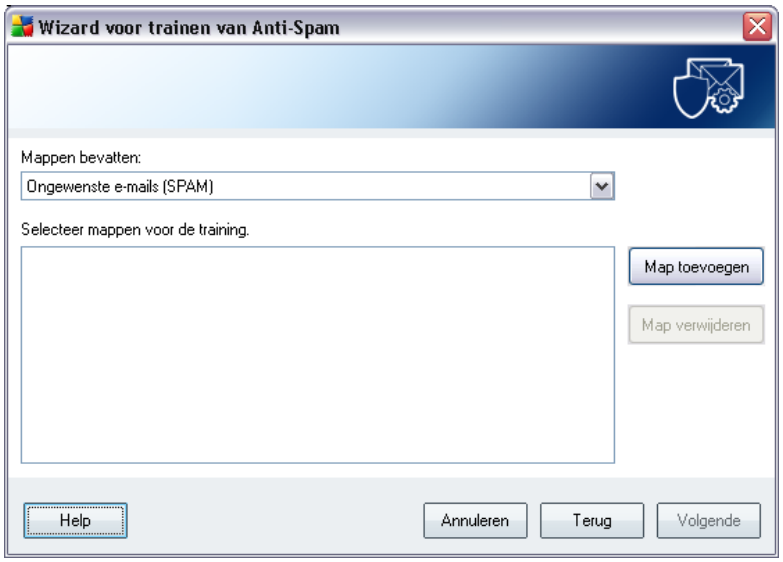
ervoor te zorgen dat u de locatie van uw map met e-mailclientberichten kent. Selecteer vervolgens ***Map met EML-bestanden*** om het pad naar die map op te geven

Het trainingsproces verloopt sneller en gemakkelijker als u de e-mails in de mappen van tevoren sorteert, zodat de map die u wilt gebruiken voor de training alleen de trainingsberichten bevat (ofwel gewenst ofwel ongewenst). Maar dat is niet noodzakelijk, omdat u de e-mails ook later in deze wizard kunt filteren.

Selecteer een optie en klik op ***Volgende*** om verder te gaan met de wizard.

De weergave van het dialoogvenster bij deze stap is afhankelijk van uw keuze hiervoor.

Mappen met EML-bestanden



Zoek in dit dialoogvenster de map met de berichten die u wilt gebruiken voor de training. Klik op de knop ***Map toevoegen*** om de map te zoeken met de .eml-bestanden (*opgeslagen e-mailberichten*). De geselecteerde map zal vervolgens in het dialoogvenster worden weergegeven.

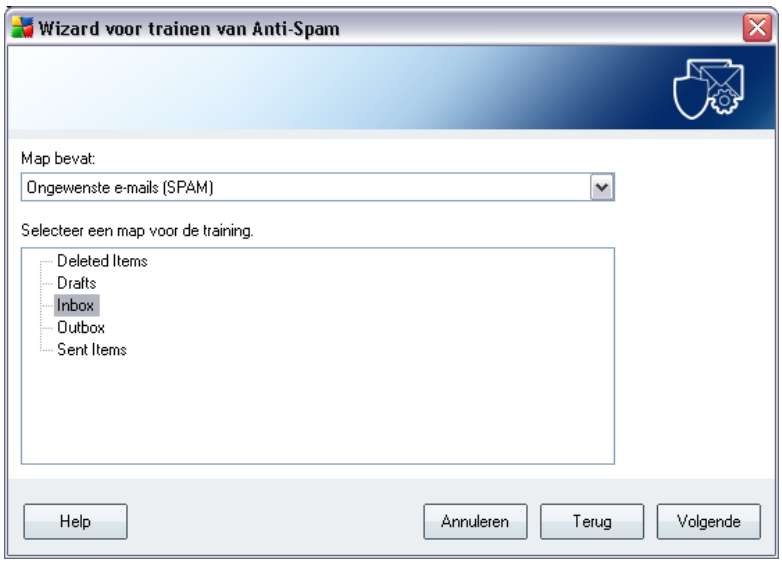
Maak met de vervolgkeuzelijst ***Mappen bevatten*** een keuze of de geselecteerde map gewenste berichten bevat (*HAM*) of ongewenste berichten (*SPAM*). NB: U kunt de berichten in de volgende stap filteren, dus de map hoeft niet uitsluitend trainingse-

mails te bevatten. U kunt ook een ongewenste selectie van mappen in de lijst ongedaan maken door te klikken op de knop ***Map verwijderen***.

Klik, als u klaar bent, op ***Volgende*** en ga verder met ***Opties voor het filteren van berichten***.

Specifieke e-mailclient

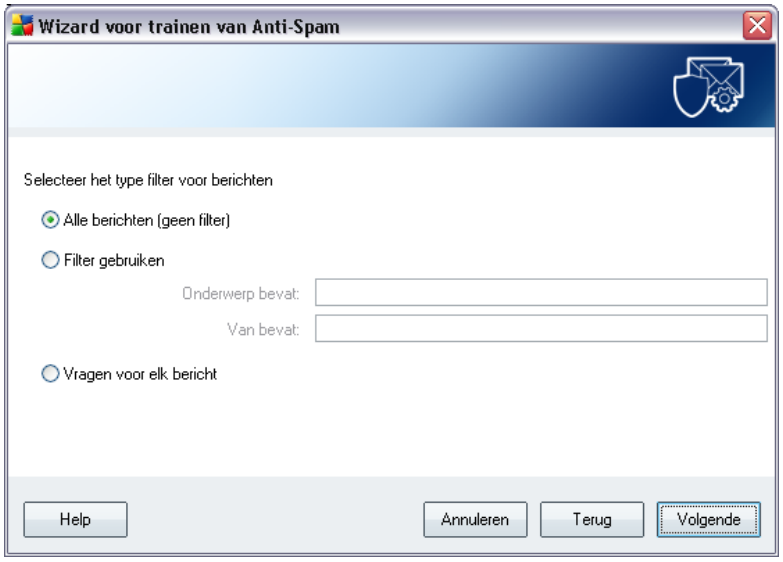
Als u een van de opties hebt bevestigd, wordt een nieuw dialoogvenster geopend.



Opmerking: *als het MS Outlook betreft, wordt u eerst gevraagd het MS Outlook-profiel te kiezen.*

Maak met de vervolgkeuzelijst ***Mappen bevatten*** een keuze of de geselecteerde map gewenste berichten bevat (*HAM*) of ongewenste berichten (*SPAM*). NB: U kunt de berichten in de volgende stap filteren, dus de map hoeft niet uitsluitend trainingse-mails te bevatten. Op het scherm staat de navigatiestructuur van de geselecteerde e-mailclient in het hoofdgedeelte van het dialoogvenster. Zoek de gewenste map in de boom en markeer deze met uw muis.

Klik, als u klaar bent, op ***Volgende*** en ga verder met ***Opties voor het filteren van berichten***.



In dit dialoogvenster kunt u de filtering instellen voor e-mailberichten.

Als u zeker weet dat de geselecteerde map alleen berichten bevat die u wilt gebruiken voor training, selecteer dan de optie ***Alle berichten (geen filtering)***.

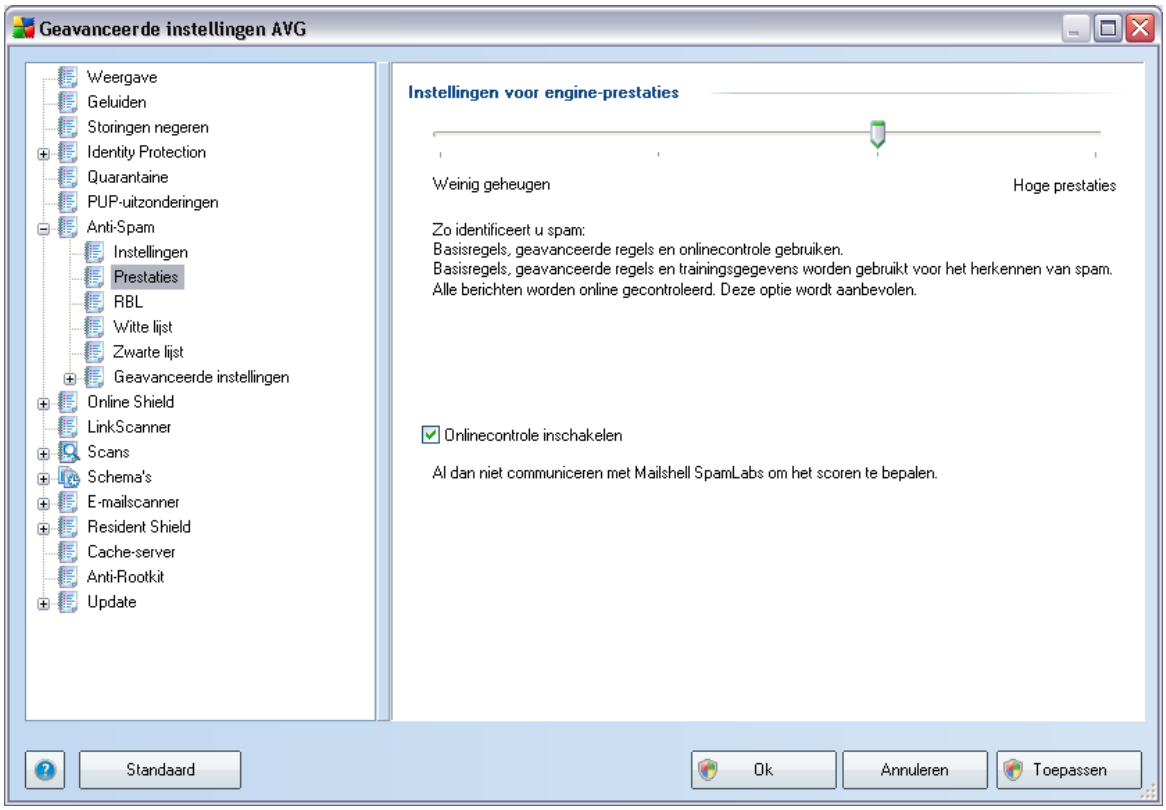
Als u niet zeker weet welke berichten in de map zitten en u wilt dat de Wizard u bij elk bericht hiernaar vraagt (zodat u kunt bepalen of u dit bericht voor training gaat gebruiken of niet), selecteert u de optie ***Voor elk bericht vragen***.

Selecteer voor meer geavanceerde filtering de optie ***Filter gebruiken***. U kunt een woord invullen (*naam*), deel van een woord of een zin waarnaar gezocht moet worden in het onderwerpveld en/of het veld van de afzender van de e-mail. Alle berichten die exact voldoen aan de ingevoerde criteria zullen worden gebruikt voor de training zonder verdere herinnering.

Let op!:*Als u beide tekstvelden invult, zullen adressen die slechts aan een van de twee voorwaarden voldoen, ook worden gebruikt.*

Als u een keuze hebt gemaakt, klikt u op ***Volgende***. Het dialoogvenster dat dan wordt geopend, heeft uitsluitend een informatieve functie en deelt mee dat de wizard klaar is om te beginnen met het verwerken van de berichten. Klik opnieuw op de knop ***Volgende*** om de training te starten. De training wordt vervolgens uitgevoerd aan de hand van de geselecteerde opties.

10.7.2. Prestaties



In het dialoogvenster ***Instellingen voor engine-prestaties*** (*dat u opent met de optie* ***Prestaties*** *in de navigatiestructuur links*) staan de instellingen voor de prestaties van het onderdeel ***Anti-Spam***. Verplaats de schuifbalk naar links of naar rechts om de scanprestaties aan te passen tussen ***Weinig geheugen*** / ***Hoge prestaties***.

- ***Weinig geheugen*** - tijdens het scanproces ter detectie van spam worden geen regels gebruikt, maar alleen trainingsgegevens. Het is niet raadzaam deze modus voor normaal gebruik te selecteren, tenzij de computerhardware van lage kwaliteit is.

- ***Hoge prestaties*** - bij deze stand wordt een groot beroep gedaan op het geheugen van de computer. Bij het scanproces ter detectie van spam worden de volgende functies gebruikt: regels en spamdatabase, basisregels, geavanceerde regels, IP-adressen van spammers en spammerdatabases.

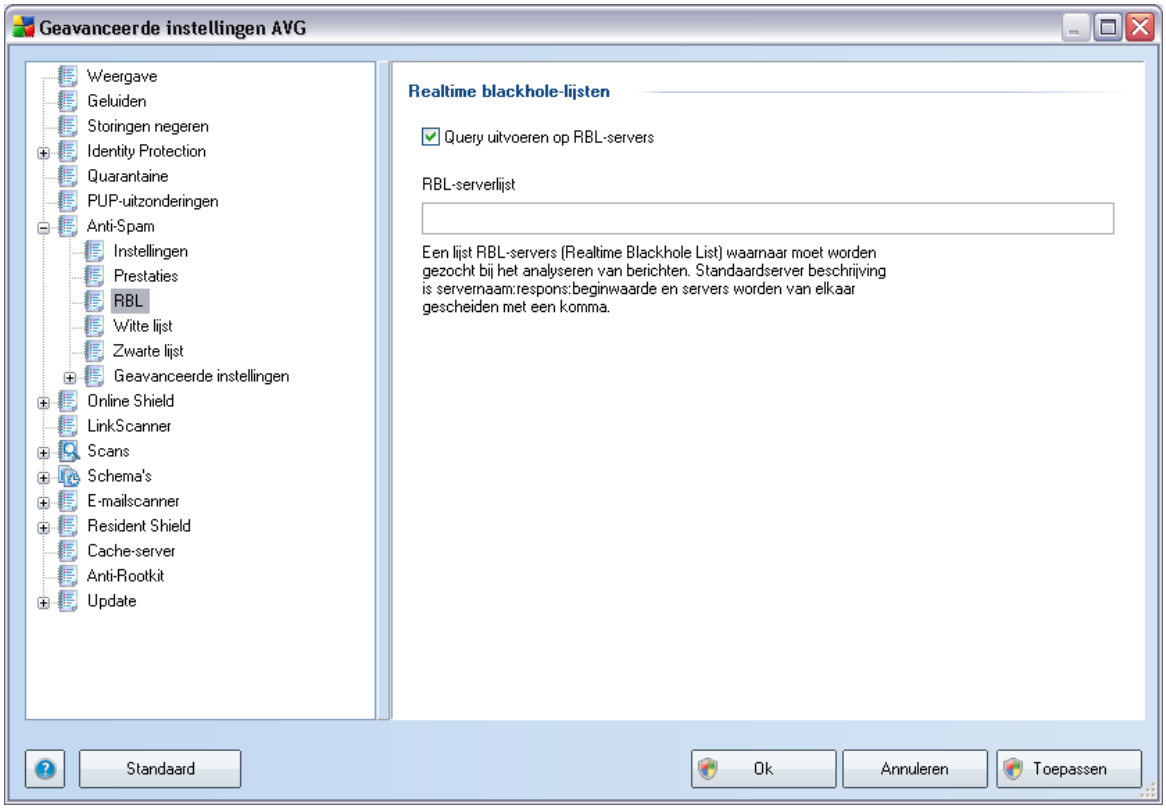
De optie ***Online controle inschakelen*** is standaard ingeschakeld. Die resulteert in een

meer precieze spamdetectie dankzij communicatie met de Mailshellservers, dat wil zeggen dat de gescande gegevens online worden vergeleken met de Mailshell database.

Over het algemeen is het raadzaam de standaardinstellingen aan te houden en die alleen te wijzigen als u daar een goede reden voor hebt. Wijzigingen aan deze configuratie moeten alleen gedaan worden door experts!

10.7.3. RBL

Met de optie ***RBL*** opent u het dialoogvenster***Realtime Blackhole Lists***:



In dit dialoogvenster kunt u de functie ***Query uitvoeren op RBL-servers*** in- en uitschakelen.

De RBL-server (*Realtime Blackhole List*) is een DNS-server met een uitgebreide database van bekende spammers. Wanneer deze functie ingeschakeld is, worden alle e-mailberichten gecontroleerd in de RBL-serverdatabase en als spam gemarkeerd wanneer ze identiek zijn aan een onderdeel van de database. De RBL-serverdatabases

bevatten de recentste spamvingerafdrukken, waardoor de beste en meest accurate spamdetectie geboden kan worden. Deze functie is vooral nuttig voor gebruikers die grote hoeveelheden spam ontvangen die normaal niet door de Anti-Spam-engine gedetecteerd wordt.

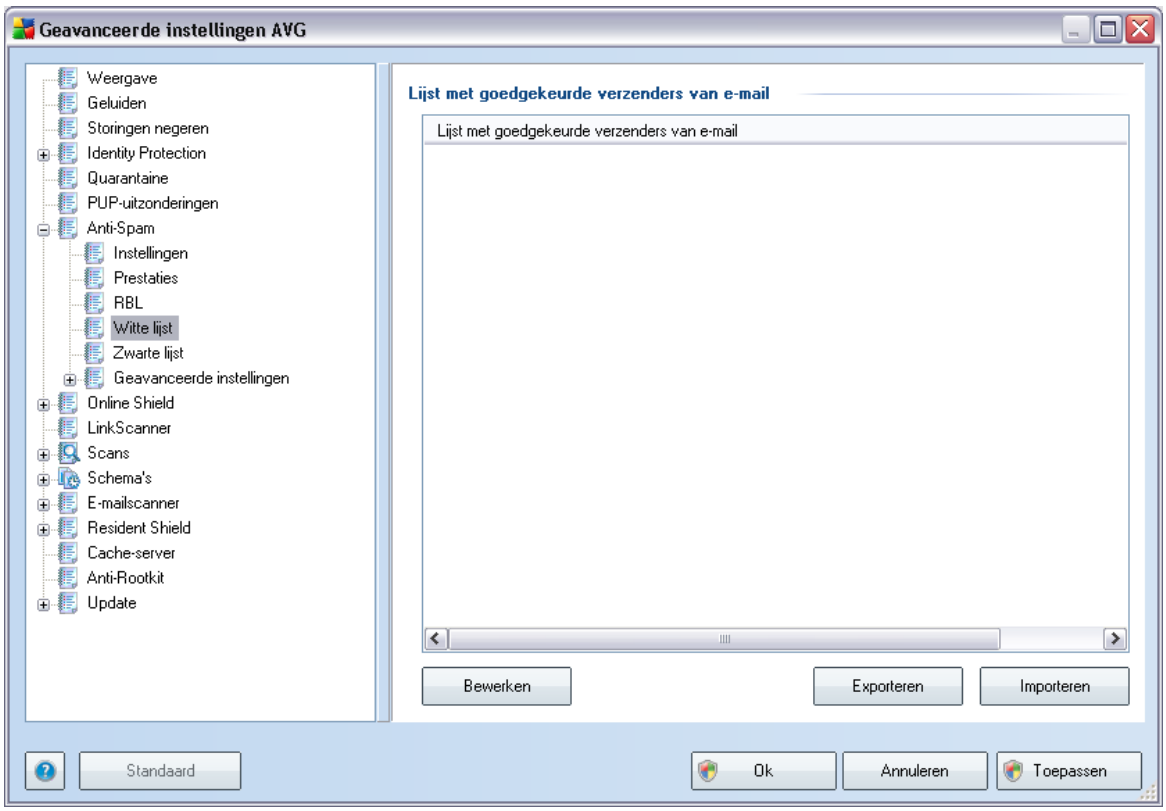
Op de ***RBL-serverlijst*** kunt u specifieke RBL-serverlocaties definiëren.

Opmerking: *Wanneer u deze functie inschakelt, worden e-mailberichten op sommige systemen en configuraties trager ontvangen, aangezien elk bericht gecontroleerd moet worden in de RBL-serverdatabase.*

Er worden geen persoonlijke gegevens naar de server verzonden!

10.7.4. Witte lijst

Met de optie ***Witte lijst*** opent u een dialoogvenster met de naam ***Lijst met goedgekeurde verzenders van e-mail***, een globale lijst met de e-mailadressen en domeinnamen van goedgekeurde afzenders. De berichten van deze afzenders zullen nooit als spam gemarkeerd worden.



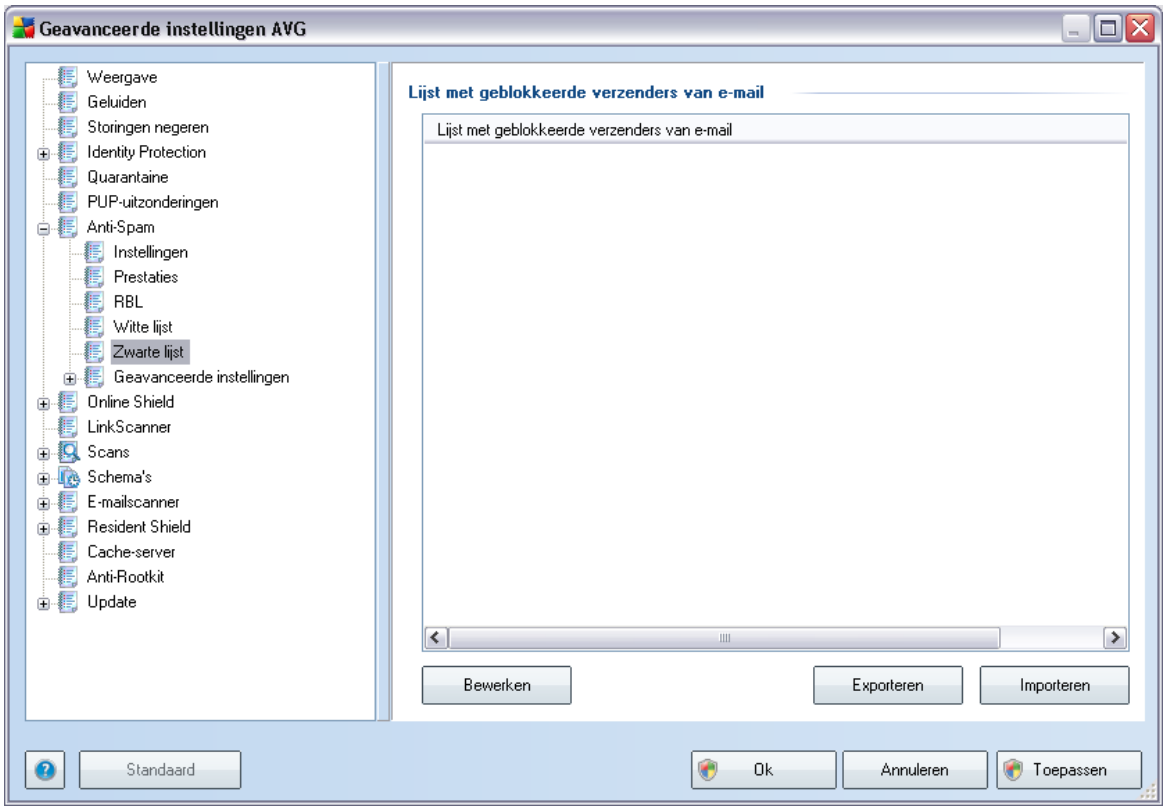
U kunt in het tekstverwerkingsgedeelte een lijst samenstellen met afzenders waarvan u zeker weet dat ze u geen ongewenste e-mail (spam) zullen sturen. U kunt ook een lijst samenstellen met domeinnamen (*bijvoorbeeld avg.com*), waarvan u weet dat ze geen spam genereren.

Als u eenmaal zo'n lijst met afzenders/domeinnamen hebt samengesteld, kunt u die op twee manieren invoeren: rechtstreeks elk e-mailadres afzonderlijk of in één keer door het importeren van de lijst. 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. Het invoerbestand moet onopgemaakte tekst bevatten en de inhoud mag niet meer dan een item (*adres, domeinnaam*) per regel bevatten.

10.7.5. Zwarte lijst

Met de optie ***Zwarte lijst*** opent u een dialoogvenster met een globale 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 waarvan 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 zo'n lijst met afzenders/domeinnamen hebt samengesteld, kunt u die op twee manieren invoeren: rechtstreeks elk e-mailadres afzonderlijk of in één keer door het importeren van de lijst. 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. Het

invoerbestand moet onopgemaakte tekst bevatten en de inhoud mag niet meer dan een item (*adres, domeinnaam*) per regel bevatten.

10.7.6. Geavanceerde instellingen

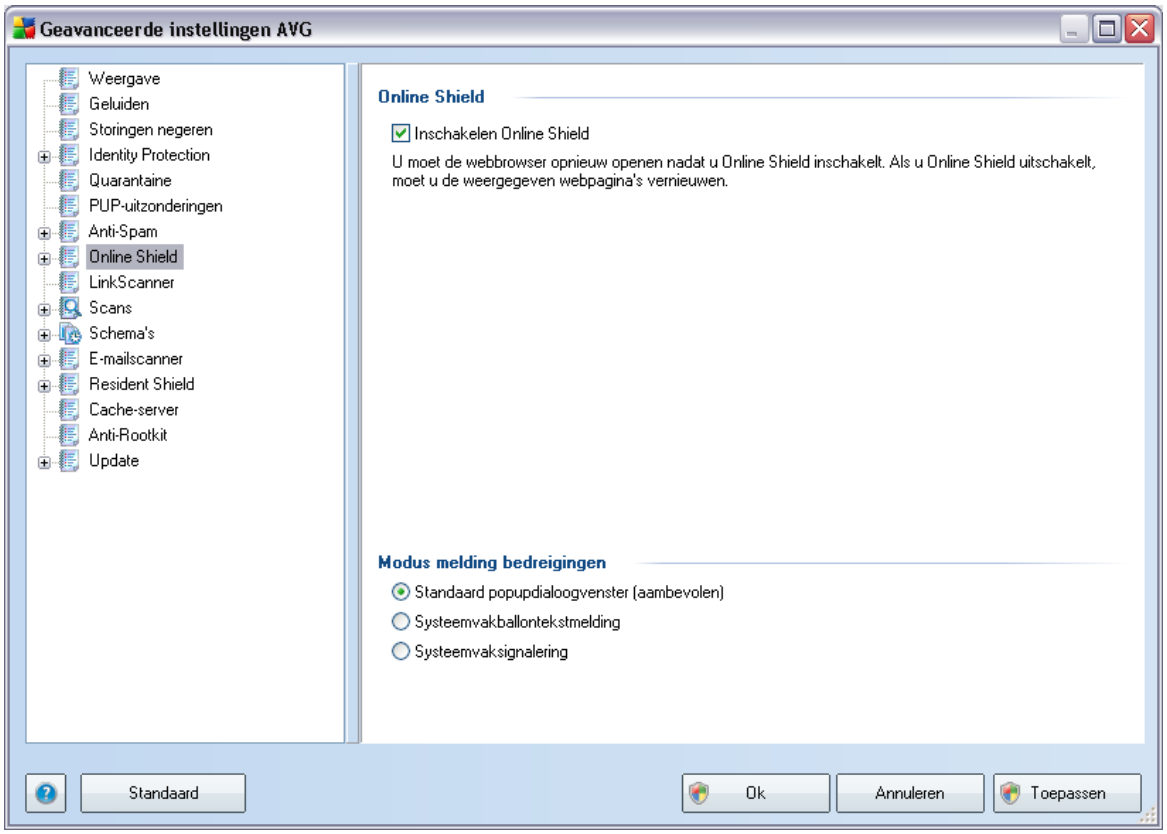
De vertakking Geavanceerde instellingen bevat uitgebreide instelopties voor het onderdeel Anti-Spam. Die instellingen zijn bedoeld voor ervaren gebruikers, met name voor netwerkbeheerders die de beveiliging tegen spam tot in details moeten configureren om e-mailservers optimaal te kunnen beschermen. Om die reden is er geen extra Help beschikbaar voor de afzonderlijke dialoogvensters; er is echter wel een korte beschrijving van elke optie direct in de gebruikersinterface.

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 ***Anti-Spam***configuratie op het geavanceerde niveau wilt wijzigen, volgt u de instructies die in de gebruikersinterface worden weergegeven. Over het algemeen is elk dialoogvenster gewijd aan één specifieke functie die u dan kunt wijzigen - de beschrijving van de functie staat steeds in datzelfde dialoogvenster:

- ***Cache*** - Vingerafdruk, Domeinreputatie, LegitRepute
- ***Training*** - max in te voeren woorden, drempel autotraining, gewicht
- ***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

10.8. Online Shield



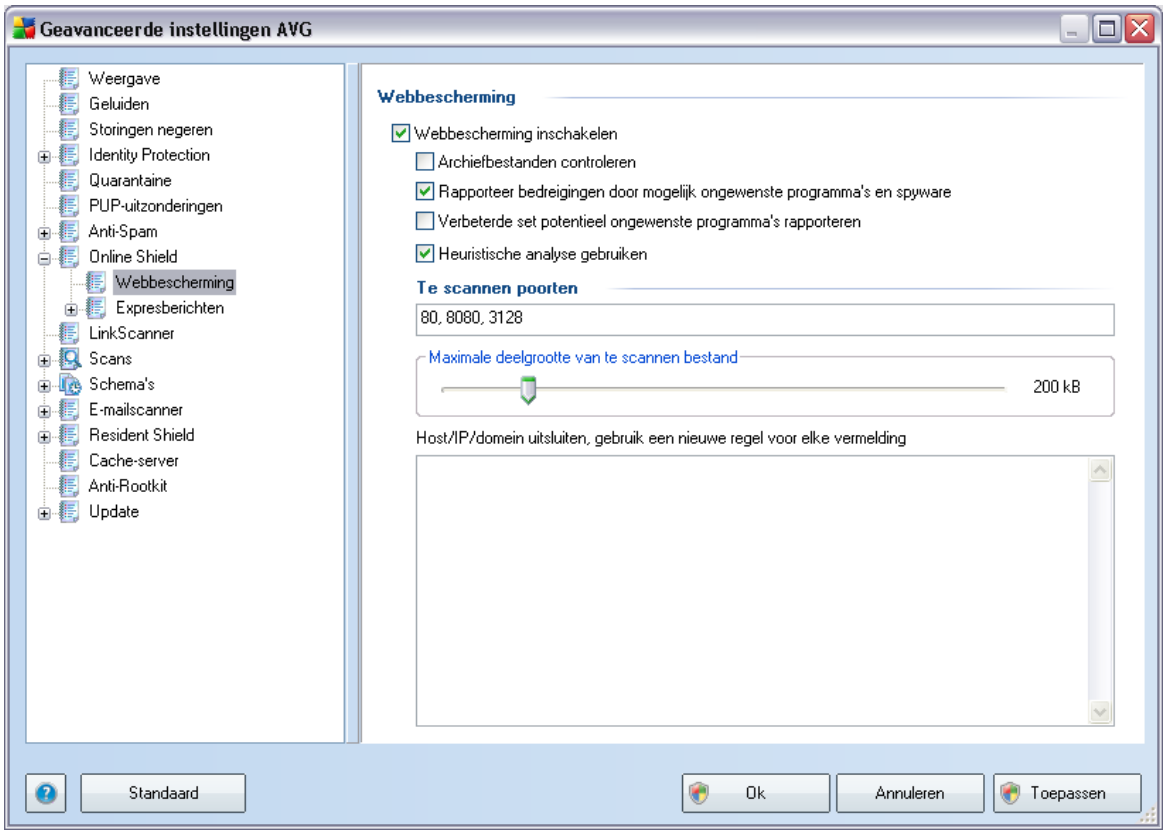
In het dialoogvenster ***Webbescherming*** kunt u het volledige onderdeel ***Online Shield*** in- en uitschakelen via de optie ***Online Shield inschakelen*** (*standaard ingeschakeld*). Voor verdere geavanceerde instellingen voor dit onderdeel verwijzen we u naar de desbetreffende dialoogvensters die in de navigatiestructuur zijn opgenomen:

- ***Webbescherming***
- ***Expresberichten***

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.

10.8.1. Webbescherming



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:

- ***Webbescherming inschakelen*** - met deze optie geeft u op of ***Online Shield*** de inhoud van webpagina's moet scannen. Ervan uitgaande dat deze optie is ingeschakeld (*standaard*), kunt u nog de volgende functies in- en uit-schakelen:
    - ***Archiefbestanden controleren*** - de inhoud van archieven scannen die zijn inbegrepen op de webpagina die u wilt weergeven.
    - ***Bedreigingen door mogelijk ongewenste programma's en spyware rapporteren*** - (*standaard ingeschakeld*): schakel dit selectievakje in om de ***Anti-Spyware***-engine te activeren en naar spyware en virussen te scannen. Spyware behoort tot een twijfelachtige categorie malware en

vormt gewoonlijk een veiligheidsrisico, maar sommige van deze programma's kunnen ook met opzet worden geïnstalleerd. Het is raadzaam deze functie niet uit te schakelen, omdat het de bescherming van uw computer vergroot.

- ***Uitgebreide sets van mogelijk ongewenste programma's rapporteren*** - als de vorige optie is geactiveerd, kunt u ook dit selectievakje inschakelen om uitgebreide pakketten van spyware te detecteren: programma's waar op zich niets aan mankeert als u ze direct van de fabrikant krijgt, maar die wel in een later stadium voor kwaadaardige praktijken kunnen worden misbruikt. 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.

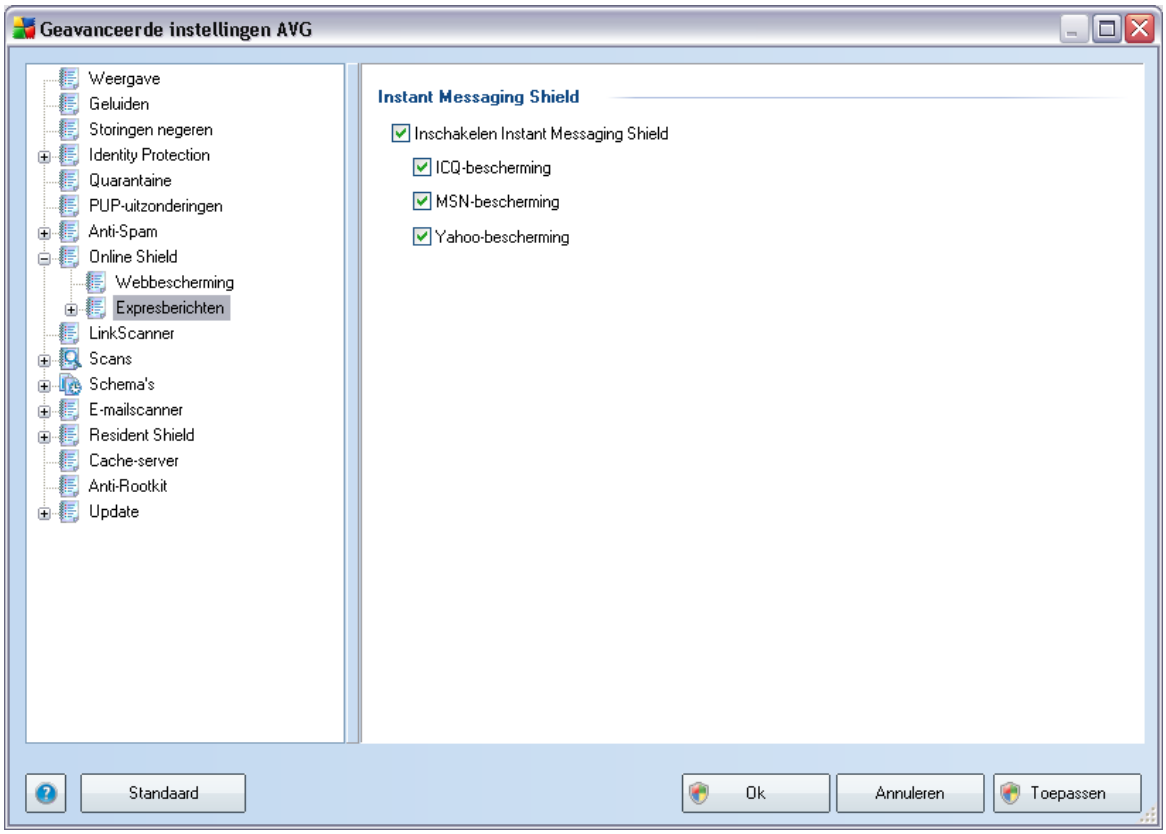
- ***Heuristische methode gebruiken*** - de inhoud scannen van een weer te geven pagina met behulp van de methode voor heuristische analyse (*dynamische emulatie van de instructies van gescande objecten in een virtuele computeromgeving*).

- ***Te scannen poorten*** - in dit vak staan de standaard poortnummers voor http-communicatie. Als u een afwijkende computerconfiguratie hebt, kunt u de poortnummers naar wens wijzigen.

- ***Maximale deelgrootte te scannen bestand*** - 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 soms veel tijd in beslag, wat het downloaden van de webpagina aanzienlijk kan vertragen. Met behulp van de schuifbalk 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: in het geval dat het bestand is geïnfecteerd, zal dat onmiddellijk worden gedetecteerd door ***Resident Shield***.

- ***Host/IP/domein uitsluiten*** - u kunt in het tekstveld de exacte naam typen van een server (*host, IP-adres, IP-adres met masker, of URL*) of een domein dat niet dient te worden gescand door ***Online Shield***. Sluit dus alleen een host uit waarvan u absoluut zeker weet dat die nooit gevaarlijke webinhoud zou leveren.

10.8.2. Expresberichten

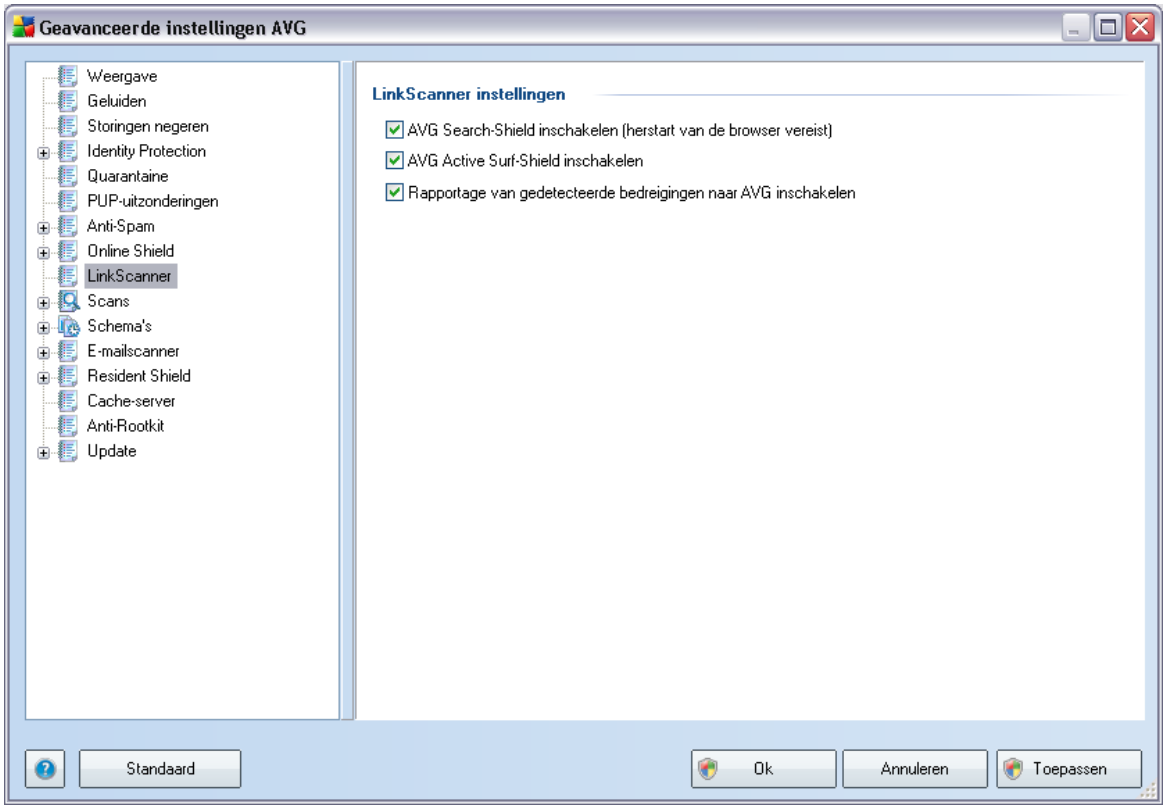


In het dialoogvenster ***Instant Messaging Shield*** kunt u de instellingen van het onderdeel ***Online Shield*** bewerken die betrekking hebben op het scannen van expresberichten. Op dit moment worden de volgende drie programma's voor expresberichten ondersteund: ***ICQ***, ***MSN*** en ***Yahoo*** - schakel het selectievakje in bij de programma's waarvoor ***de online communicatie moet bewaken.***

Voor het specificeren van toegestane/geblokkeerde gebruikers kunt u de bij de programma's horende dialoogvensters (***Geavanceerd ICQ***, ***Geavanceerd MSN,*** ***Geavanceerd Yahoo***) openen en de ***Witte lijst*** (*lijst met gebruikers die u toelaat voor communicatie*) en de ***Zwarte lijst (***(*lijst met gebruikers die moeten worden geblokkeerd*) invullen.

10.9. LinkScanner

In het dialoogvenster ***Instellingen LinkScanner*** kunt u de basisfuncties van ***LinkScanner*** in- en uitschakelen:



- ***AVG Search-Shield inschakelen*** - (*standaard ingeschakeld*): pictogrammen met een indicatie bij de resultaten van zoekopdrachten met Google, Yahoo!, Bing, Yandex, Altavista of Baidu die wordt verkregen door vooraf de inhoud van sites die door de zoekmachine worden geretourneerd, te controleren.

- ***AVG Active Surf-Shield inschakelen*** - (*standaard ingeschakeld*): actieve (*real-time*) bescherming tegen websites met exploits op het moment dat ze worden geadresseerd. Als zodanig bekend staande kwaadaardige sites en de inhoud met exploits worden geblokkeerd op het moment dat de gebruiker ze adresseert in de browser (*of met een andere toepassing die HTTP gebruikt*).

- ***Rapportage van gedetecteerde bedreigingen naar AVG inschakelen*** - (*standaard ingeschakeld*): schakel dit selectievakje in voor rapportage van

exploits en kwaadaardige sites waarmee gebruikers via ***AVG Active Surf-Shield*** of ***AVG Search-Shield*** zijn geconfronteerd, naar de database waarin gegevens worden verzameld over kwaadaardige praktijken op internet.

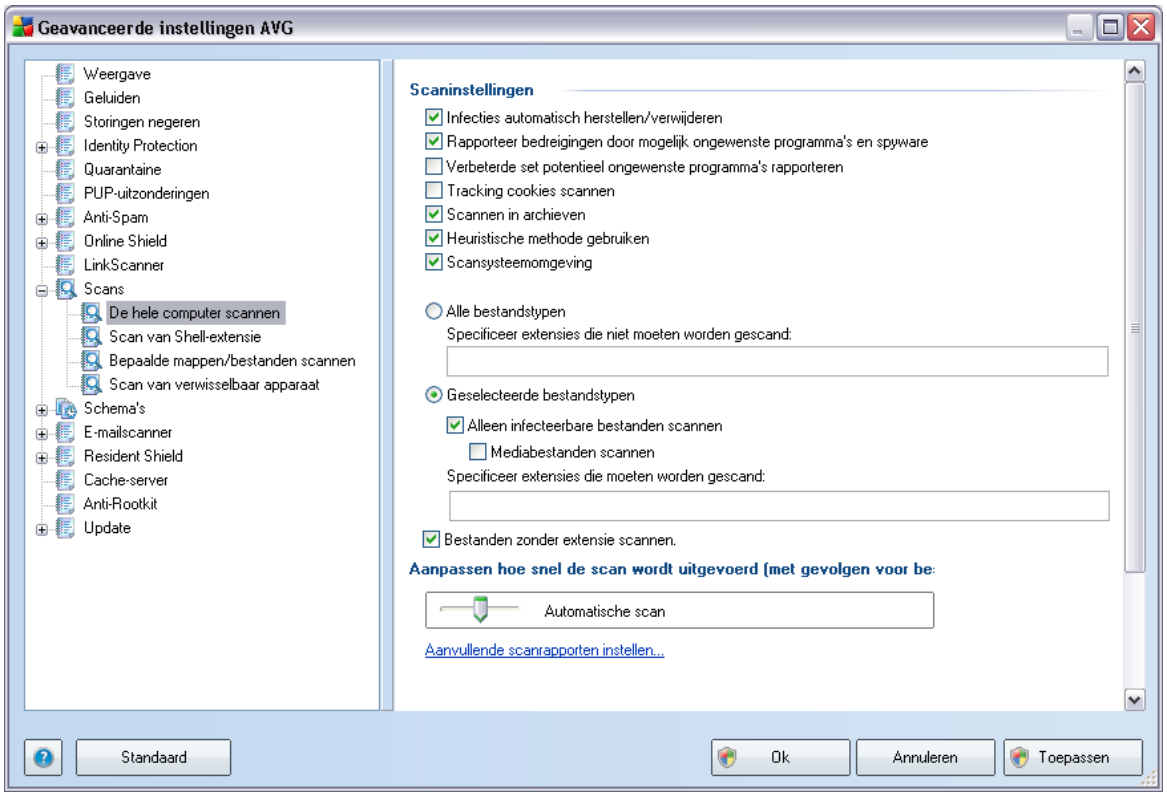
10.10. Scans

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

- ***Volledige computer scannen*** - vooraf gedefinieerde standaardscan waarbij de hele computer wordt gescand
- ***Shell-extensie scannen*** - scannen van een specifiek object direct in de Windows Verkenner
- ***Bepaalde mappen of bestanden scannen*** - vooraf gedefinieerde standaardscan waarbij een geselecteerd gedeelte van de computer wordt gescand
- ***Scan van verwisselbaar apparaat*** - scannen van verwisselbare apparaten die op de computer worden aangesloten

10.10.1. De hele computer scannen

Met de optie ***De hele computer scannen*** opent u een dialoogvenster waarin u de parameters kunt aanpassen van één van de vooraf door de leverancier gedefinieerde scans, namelijk ***Volledige computer scannen***:



Scaninstellingen

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

- ***Infecties automatisch herstellen/verwijderen*** - 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 ***Quarantaine*** verplaatst.
- ***Bedreigingen door mogelijk ongewenste programma's en spyware rapporteren*** - (*standaard ingeschakeld*): schakel dit selectievakje in om de ***Anti-Spyware***-engine te activeren en naar spyware en virussen te scannen. Spyware behoort tot een twijfelachtige categorie malware en vormt gewoonlijk een veiligheidsrisico, maar sommige van deze programma's kunnen ook met opzet worden geïnstalleerd. Het is raadzaam deze functie niet uit te schakelen, omdat het de bescherming van uw computer vergroot.

- ***Uitgebreide sets van mogelijk ongewenste programma's rapporteren*** - als de vorige optie is geactiveerd, kunt u ook dit selectievakje inschakelen om uitgebreide pakketten van spyware te detecteren: programma's waar op zich niets aan mankeert als u ze direct van de fabrikant krijgt, maar die wel in een later stadium voor kwaadaardige praktijken kunnen worden misbruikt. 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.

- ***Tracking cookies scannen*** - deze parameter van het onderdeel Anti-Spyware 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*** - met deze parameter bepaalt u of alle bestanden moeten worden gescand, ook die bestanden die zijn gecomprimeerd in archiefbestanden, bijv. ZIP, RAR, ...

- ***Heuristische methode gebruiken***- 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;

- ***Systeemgebieden scannen*** - bij het scannen worden ook de systeemgebieden van de computer betrokken.

Geef op wat u precies wilt scannen

- ***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 mogelijk 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, reduceert 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 aan de hand 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

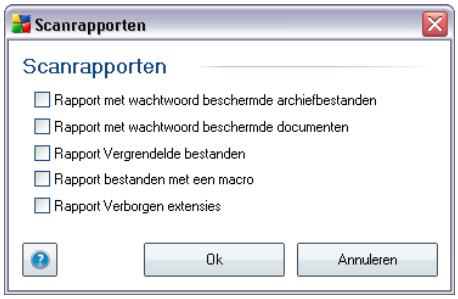
houden, tenzij u een goede reden hebt om die te wijzigen. Bestanden zonder extensie zijn uitermate verdacht en dienen altijd te worden gescand.

Prioriteit scanproces

In het gedeelte ***Prioriteit scanproces*** kunt u nader specificeren hoe snel moet worden gescand in samenhang met het beroep dat wordt gedaan op o.a. het werkgeheugen van uw computer (systeembronnen). Standaard is deze optie ingesteld op een gemiddeld niveau van gebruik van systeembronnen. Als u sneller wilt scannen, duurt het scannen minder lang, maar wordt een aanzienlijk groter beslag gelegd op o.a. het werkgeugen tijdens het scannen, zodat andere activiteiten op de computer trager zullen verlopen (*u kunt deze optie inschakelen als er verder niemand van de pc gebruikmaakt*). U kunt echter het beroep op o.a. het werkgeheugen ook verkleinen door te kiezen voor een langere scanduur.

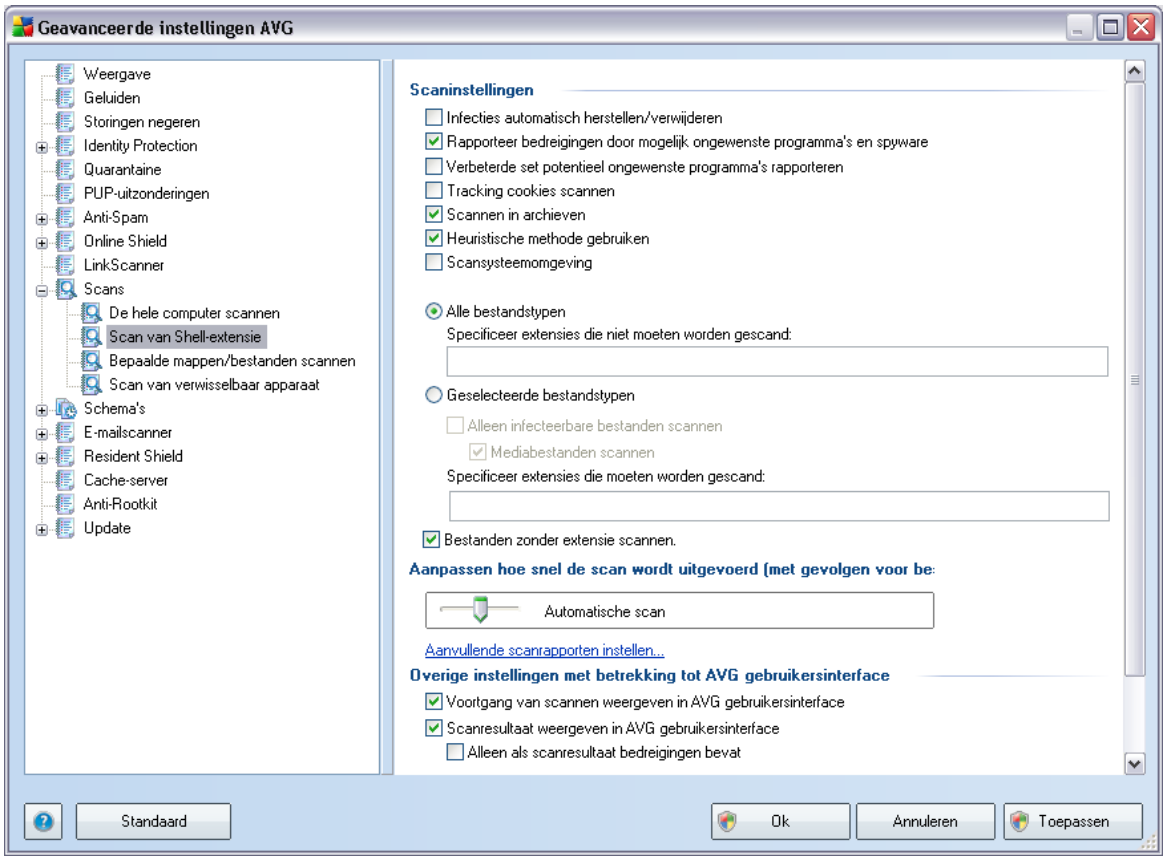
Aanvullende scanrapporten instellen...

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:



10.10.2. Shell-extensie scannen

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

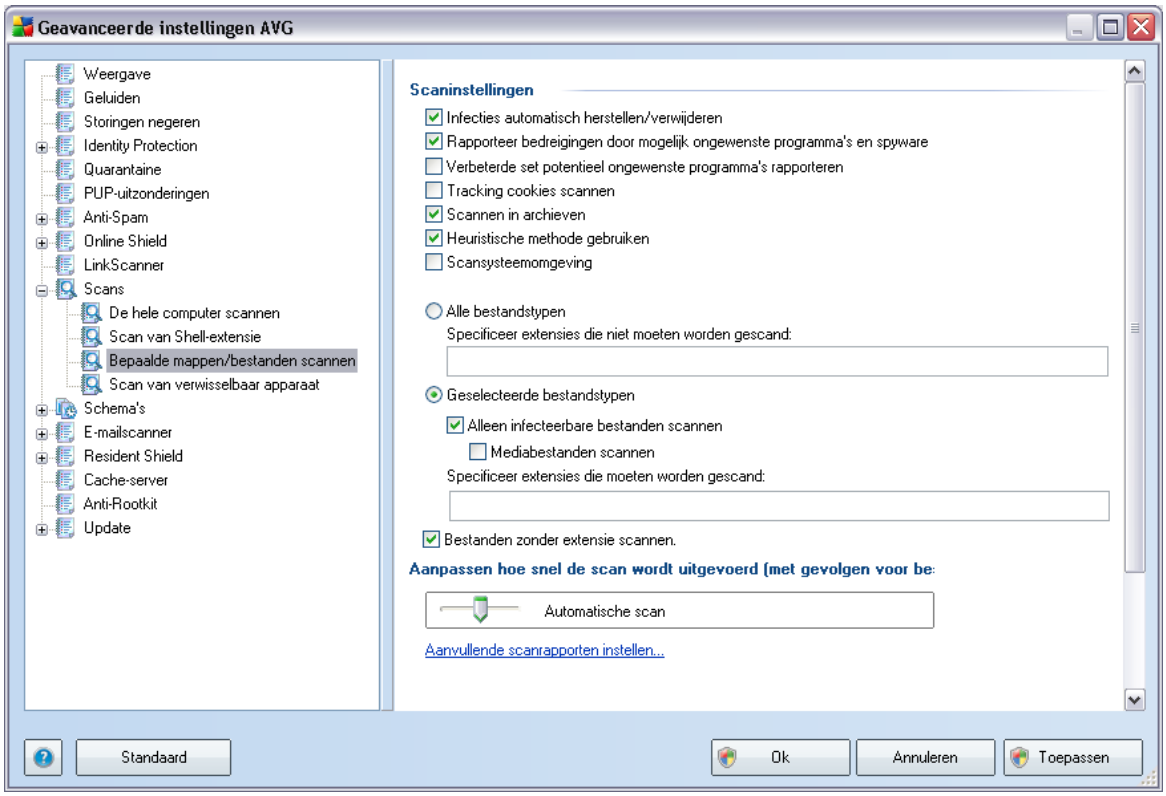


De lijst met beschikbare parameters is dezelfde als die van ***De hele computer scannen***. De standaardinstellingen verschillen echter wel: bij ***De hele computer scannen*** zijn de meeste parameters geselecteerd, terwijl bij ***Scan van Shell-extensie*** (***Scannen in Windows Verkenner***) alleen de relevante parameters zijn ingeschakeld.

Opmerking: *Zie het hoofdstuk* ***Geavanceerde instellingen AVG / Scans / Volledige computer scannen*** *voor een beschrijving van specifieke parameters.*

10.10.3. Bepaalde mappen of bestanden scannen

Het dialoogvenster voor het bewerken van de instellingen voor ***Bepaalde mappen of bestanden scannen*** is identiek aan het dialoogvenster voor het bewerken van instellingen voor ***Volledige computer scannen***. Alle configuratie-opties zijn hetzelfde, al zijn de standaardinstellingen voor ***Volledige computer scannen*** strikter:

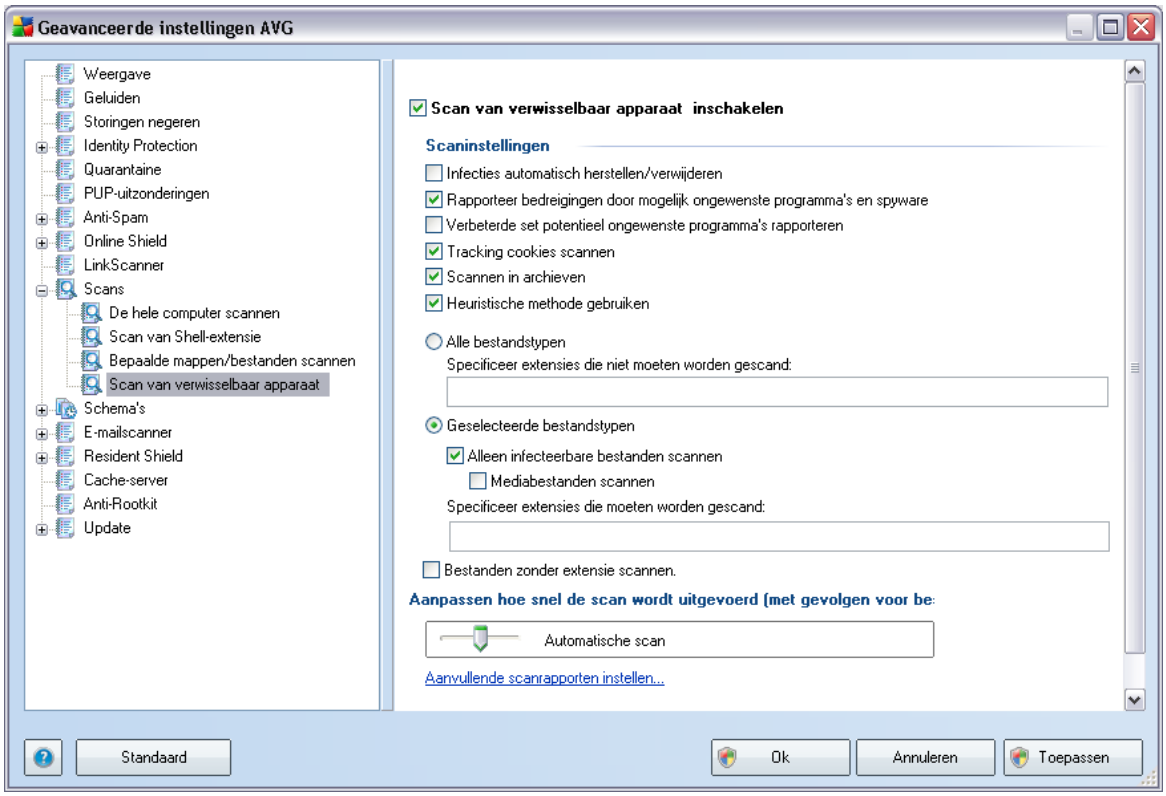


Alle parameters die u instelt in dit configuratiedialoogvenster hebben alleen betrekking op het scannen met de optie ***Bepaalde mappen of bestanden scannen***!

Opmerking: *Zie het hoofdstuk* ***Geavanceerde instellingen AVG / Scans / Volledige computer scannen*** *voor een beschrijving van specifieke parameters.*

10.10.4. 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 ***Volledige computer scannen***:



De ***Scan van verwisselbaar apparaat*** wordt automatisch uitgevoerd wanneer u een verwisselbaar aparaat 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 deze vorm van scannen bij de hand te houden en de scan wanneer noodzakelijk automatisch uit te voeren, schakelt u het selectievakje ***Scan van verwisselbaar apparaat inschakelen*** in.

Opmerking: *Zie het hoofdstuk* ***Geavanceerde instellingen AVG / Scans / Volledige computer scannen*** *voor een beschrijving van specifieke parameters.*

10.11. Schema's

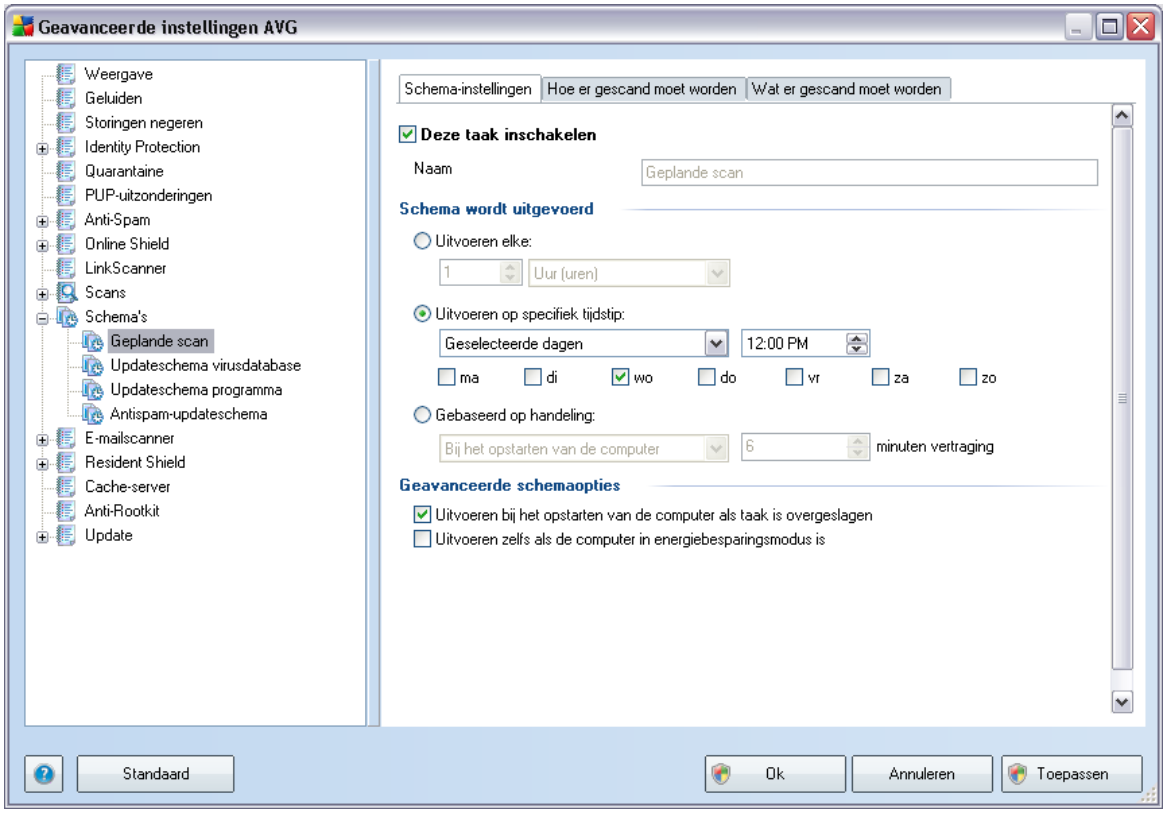
In het gedeelte ***Schema's*** kunt u de standaardinstellingen bewerken van:

- Schema volledige computer scannen
- Updateschema virusdatabase

- Updateschema programma
- Updateschema Anti-Spam

10.11.1. Geplande scan

U kunt op drie tabbladen parameters instellen voor het schema van de geplande scan (*of een nieuw schema opstellen*):



Op het tabblad ***Taakinstellingen*** kunt u eerst het selectievakje ***Deze taak inschakelen*** uitschakelen als u de geplande test tijdelijk niet wilt uitvoeren, en weer inschakelen als de noodzaak daarvoor zich aandient.

In het tekstveld ***Naam*** (*bij alle standaardschema's uitgeschakeld*) staat de naam die door de leverancier van het programma aan het schema is toegewezen. U kunt een nieuw schema dat u toevoegt, zelf een naam geven (*klik met de rechtermuisknop op het item* ***Geplande scan*** *in de navigatiestructuur links om een nieuw schema toe te*

voegen); in dat geval kunt u die naam in het tekstveld bewerken. Probeer altijd korte, maar niettemin veelzeggende namen te gebruiken voor scans zodat u ze achteraf te midden van andere scans kunt herkennen.

Voorbeeld: *het is niet handig om een scan als naam "nieuwe scan" of "mijn scan" te geven, omdat die namen geen aanduiding geven van 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 Bepaalde mappen of bestanden scannen.*

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

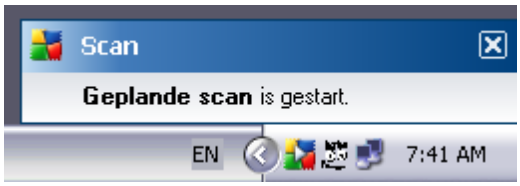
Schema wordt uitgevoerd

Hier kunt u tijdsintervallen opgeven waarmee de nieuwe geplande scan moet worden uitgevoerd. U kunt deze interval op verschillende manieren definiëren: als een steeds terugkerende scan die na verloop van een bepaalde tijd (***Uitvoeren elke ...***) moet worden uitgevoerd, als scan die op een bepaalde datum en een bepaald tijdstip (***Uitvoeren met een bepaalde tussentijd...***) moet worden uitgevoerd, of door een gebeurtenis te definiëren waaraan het uitvoeren van de scan moet worden gekoppeld (***Actie bij het opstarten van de computer***).

Geavanceerde schemaopties

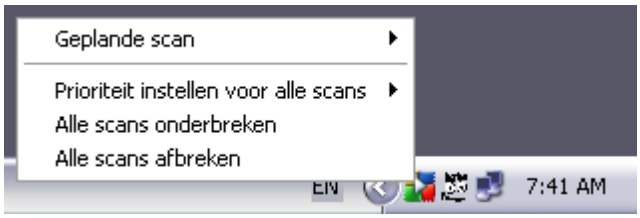
In deze sectie kunt u bepalen onder welke omstandigheden de scan wel of niet moet worden uitgevoerd als de computer in een energiebesparingsmodus is of helemaal is uitgeschakeld.

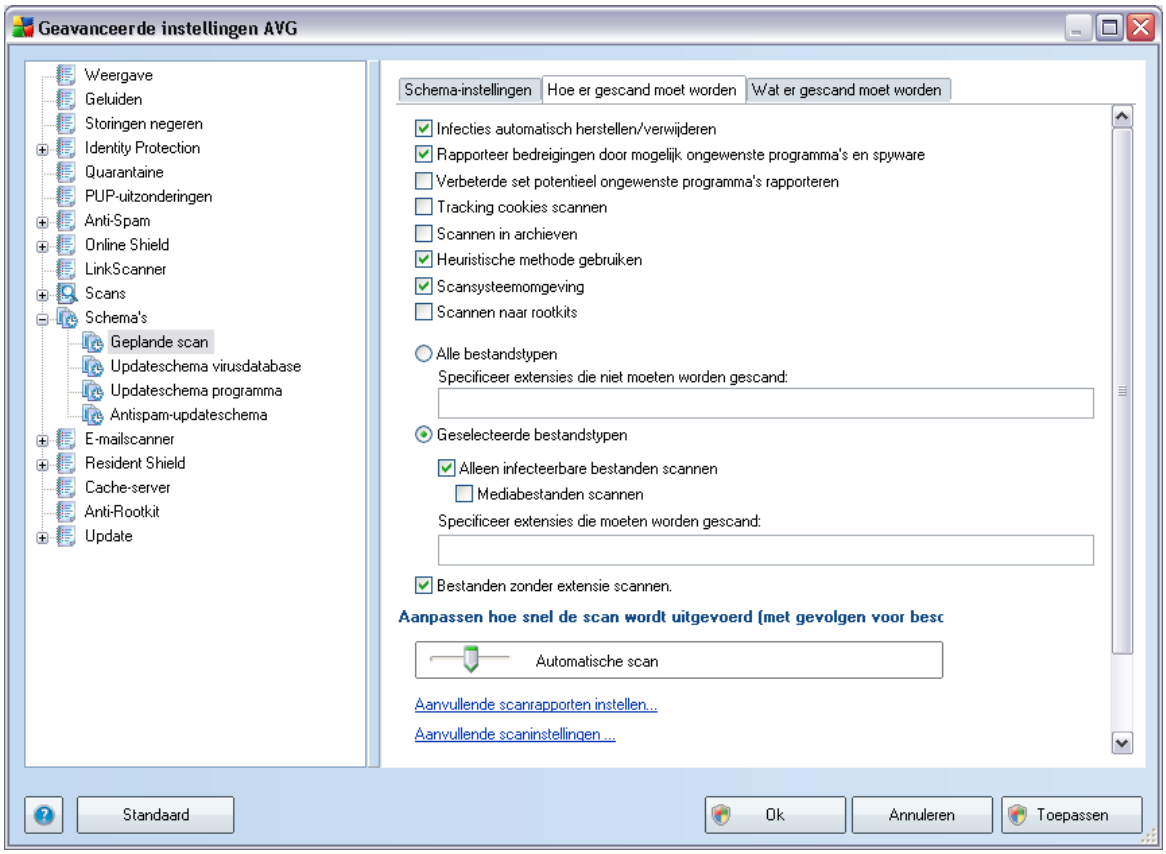
Zodra de geplande scan is gestart op het tijdstip dat u hebt opgegeven, wordt u hierover geïnformeerd via een pop-upvenster dat wordt geopend boven het systeemvakpictogram van AVG:



Vervolgens verschijnt er een nieuw systeemvakpictogram van AVG (*in kleur met een witte pijl - zie afbeelding hierboven*) 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 contextmenu te openen waarin u kunt besluiten om de huidige scan te onderbreken of zelfs te beëindigen:





Op het tabblad ***Hoe er gescand moet worden*** staat een lijst met scanparameters die kunnen worden in- en uitgeschakeld. Standaard zijn de meeste parameters ingeschakeld en wordt de desbetreffende 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:

- ***Infecties automatisch herstellen/verwijderen*** - 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 ***Quarantaine*** verplaatst.

- ***Bedreigingen door mogelijk ongewenste programma's en spyware rapporteren*** - (*standaard ingeschakeld*): schakel dit selectievakje in om de ***Anti-Spyware***-engine te activeren en naar spyware en virussen te scannen. Spyware behoort tot een twijfelachtige categorie malware en vormt gewoonlijk een veiligheidsrisico, maar sommige van deze programma's kunnen ook met opzet worden geïnstalleerd. Het is raadzaam deze functie niet uit te schakelen, omdat het de bescherming van uw computer vergroot.

- ***Uitgebreide sets van mogelijk ongewenste programma's rapporteren*** - als de vorige optie is geactiveerd, kunt u ook dit selectievakje inschakelen om uitgebreide pakketten van spyware te detecteren: programma's waar op zich niets aan mankeert als u ze direct van de fabrikant krijgt, maar die wel in een later stadium voor kwaadaardige praktijken kunnen worden misbruikt. 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.

- ***Tracking cookies scannen***- (*standaard ingeschakeld*): deze parameter van het onderdeel ***Anti-Spyware*** 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 elektronische winkelwagentjes*)

- ***Scannen binnen archieven*** - (*standaard ingeschakeld*): deze parameter bepaalt of bij het scannen alle bestanden moeten worden gecontroleerd, ook als die op de een of andere manier zijn gecomprimeerd, bijv. ZIP, RAR, ...

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

- ***Systeemgebieden scannen*** - (*standaard ingeschakeld*): als de parameter is ingeschakeld worden ook de systeemgebieden gescand;

- ***Scannen naar rootkits*** - schakel dit selectievakje in als u rootkitdetectie wilt opnemen in uw scan van de hele computer. Rootkitdetectie is afzonderlijk beschikbaar in het onderdeel ***Anti-Rootkit;***

Geef op wat u precies wilt scannen

- ***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 mogelijk 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, reduceert 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 aan de hand van extensies opgeven welke bestanden altijd moeten worden gescand.

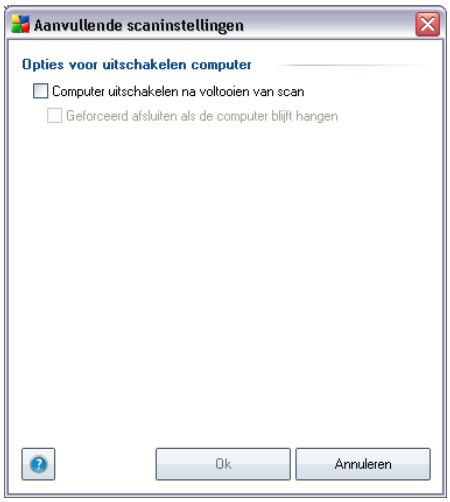
- U kunt bovendien aangeven of u ***bestanden zonder extensie wilt scannen*** - Deze optie is standaard ingeschakeld en we raden u aan deze instelling aan te houden, tenzij u een goede reden hebt om die te wijzigen. Bestanden zonder extensie zijn uitermate verdacht en dienen altijd te worden gescand.

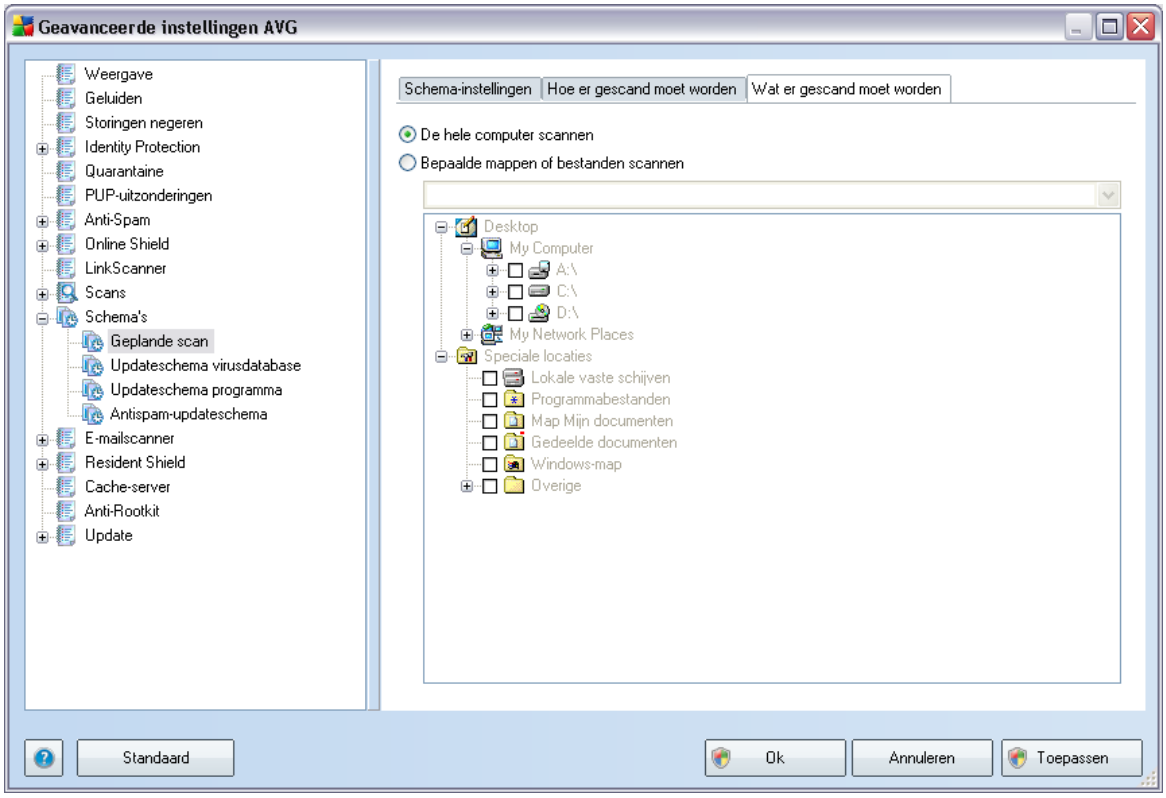
Prioriteit scanproces

In het gedeelte ***Prioriteit scanproces*** kunt u nader specificeren hoe snel moet worden gescand in samenhang met het beroep dat wordt gedaan op o.a. het werkgeheugen van uw computer (systeembronnen). Standaard is deze optie ingesteld op een gemiddeld niveau van gebruik van systeembronnen. Als u sneller wilt scannen, duurt het scannen minder lang, maar wordt een aanzienlijk groter beslag gelegd op o.a. het werkgeheugen tijdens het scannen, zodat andere activiteiten op de computer trager zullen verlopen (*u kunt deze optie inschakelen als er verder niemand van de pc gebruikmaakt*). U kunt echter het beroep op o.a. het werkgeheugen ook verkleinen door te kiezen voor een langere scanduur.

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:

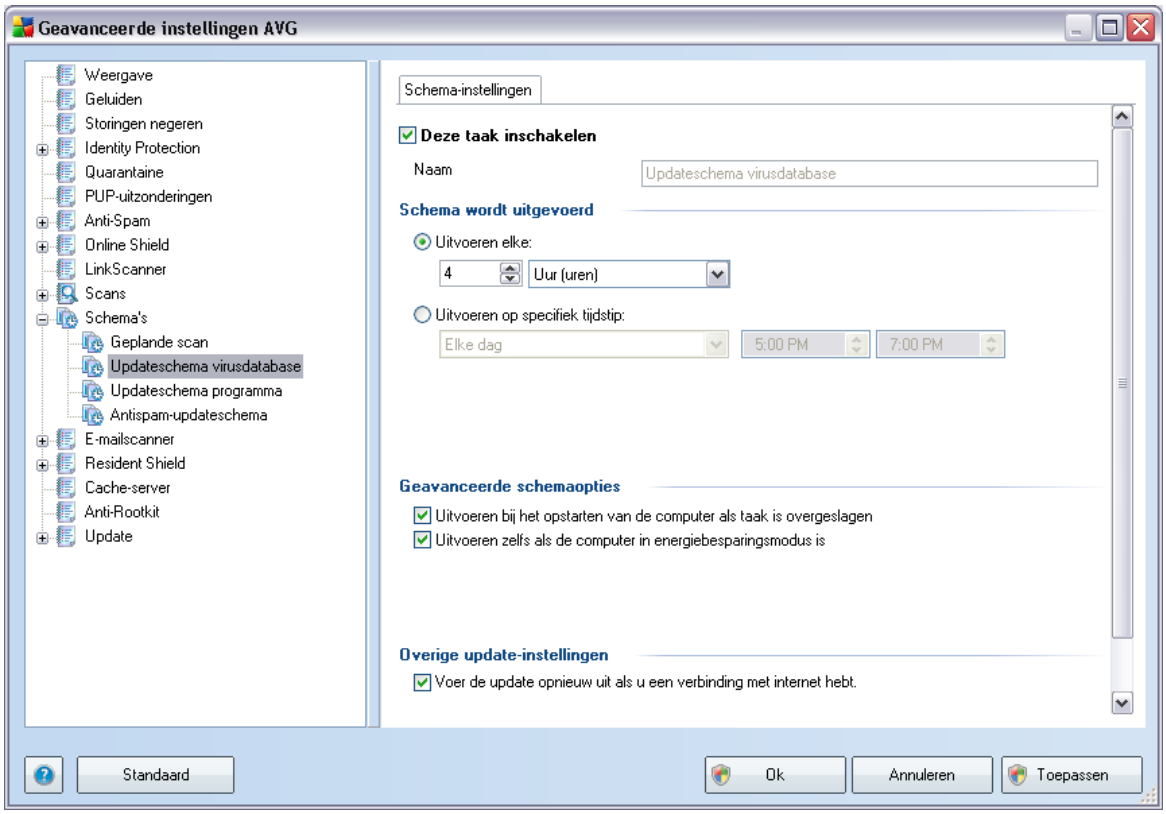
Klik op ***Aanvullende scaninstellingen...*** om een nieuw dialoogvenster ***Opties voor uitschakelen computer***te openen waarin u kunt opgeven of de computer automatisch moet worden afgesloten zodra het scannen is voltooid. Als u die optie bevestigt (***Computer afsluiten na voltooien van scanproces***), 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***).





Op het tabblad ***Wat er gescand moet worden*** kunt u opgeven welke scan moet worden uitgevoerd: een scan van de hele computer of een scan van specifieke 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.

10.11.2. Updateschema virusdatabase



Op het tabblad ***Taakinstellingen*** kunt u eerst het selectievakje ***Deze taak inschakelen*** uitschakelen als u de geplande update van de virusdatabase tijdelijk niet wilt uitvoeren, en weer inschakelen als de noodzaak daarvoor zich aandient. Elementaire planning van updates voor de virusdatabase wordt beheerd met het onderdeel ***Updatebeheer***. In dat dialoogvenster kunt u gedetailleerde parameters instellen voor het updateschema. In het tekstveld ***Naam*** (*bij alle standaardschema's uitgeschakeld*) staat de naam die door de leverancier van het programma aan het schema is toegewezen.

Schema wordt uitgevoerd

In dit gedeelte geeft u de tijdsintervallen op waarmee het nieuwe virusdatabase-updateschema moet worden uitgevoerd. 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.

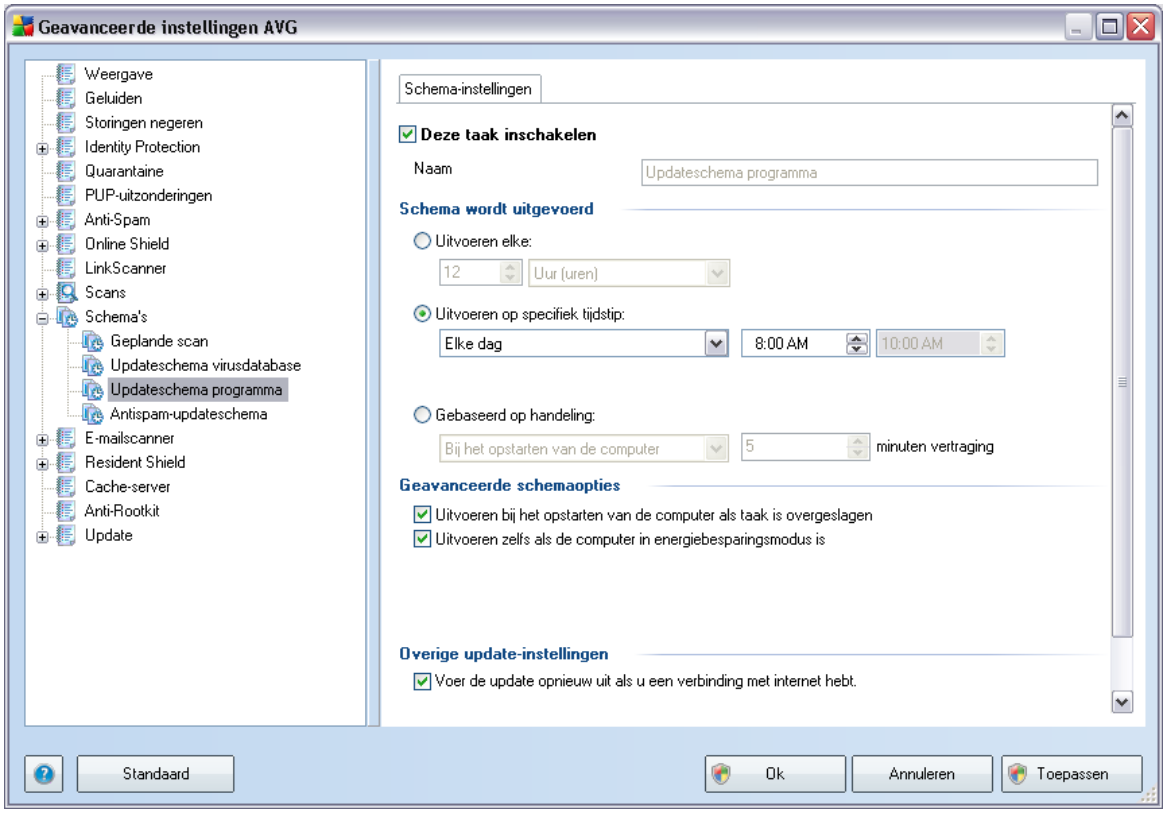
Geavanceerde schemaopties

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

Overige update-instellingen

Schakel tot slot het selectievakje in bij ***Voer de update opnieuw uit zodra de internetverbinding beschikbaar is*** om ervoor te zorgen dat, als de internetverbinding verbroken wordt en de updateprocedure mislukt, die onmiddellijk weer opnieuw zal worden uitgevoerd na herstel van de internetverbinding.

Zodra de geplande update wordt gestart op de tijd die u hebt gespecificeerd, ontvangt u hierover een bericht via een pop-upvenster dat wordt geopend boven het AVG systeemvakpictogram (*mits u de standaardconfiguratie van het dialoogvenster* ***Geavanceerde instellingen/Weergave*** *ongewijzigd hebt gelaten)*.



Op het tabblad ***Taakinstellingen*** kunt u eerst het selectievakje ***Deze taak inschakelen*** uitschakelen als u de geplande programma-update tijdelijk niet wilt uitvoeren, en weer inschakelen als de noodzaak daarvoor zich aandient. In het tekstveld ***Naam*** (*bij alle standaardschema's uitgeschakeld*) staat de naam die door de leverancier van het programma aan het schema is toegewezen.

Schema wordt uitgevoerd

Geef een tijdsinterval op waarmee de nieuwe programma-update moet worden uitgevoerd. U kunt deze 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 (***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.

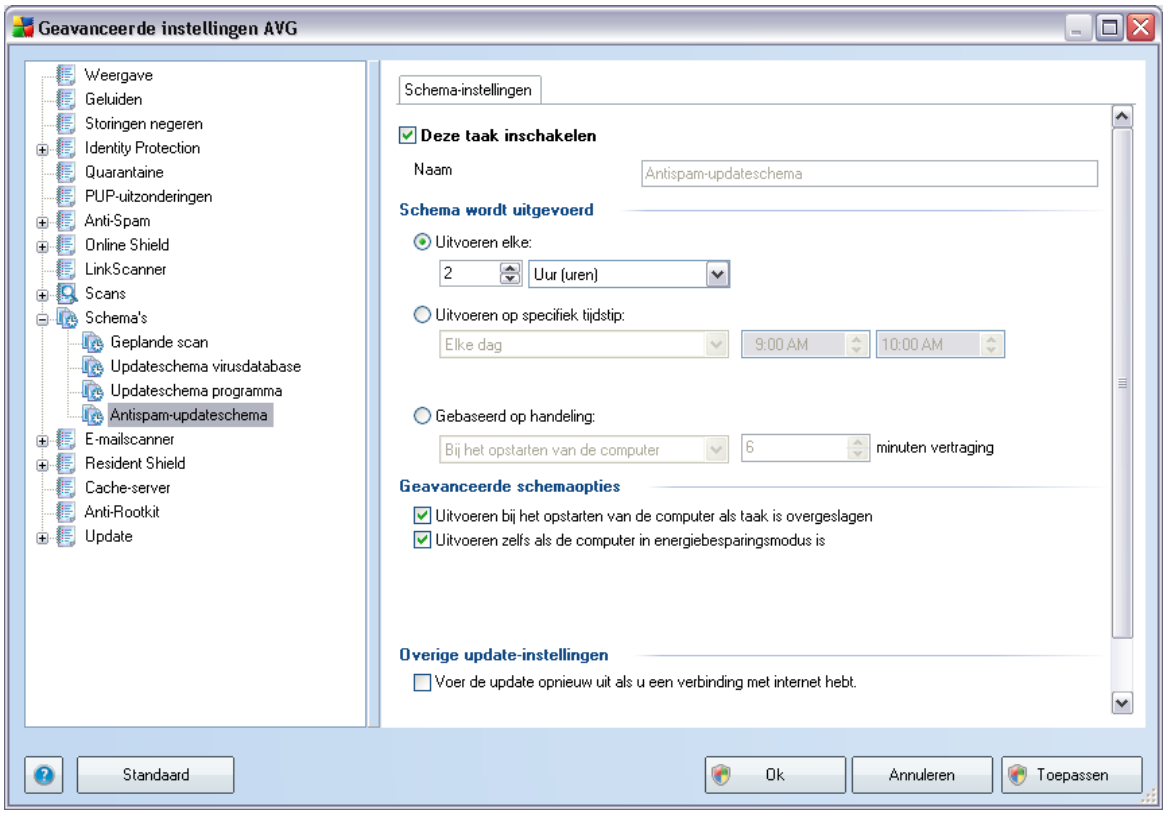
Overige update-instellingen

Schakel het selectievakje in bij ***Voer de update opnieuw uit zodra de internetverbinding beschikbaar is*** om ervoor te zorgen dat, als de internetverbinding verbroken wordt en de updateprocedure mislukt, die onmiddellijk weer opnieuw zal worden uitgevoerd na herstel van de internetverbinding.

Zodra de geplande update wordt gestart op de tijd die u hebt gespecificeerd, ontvangt u hierover een bericht via een pop-upvenster dat wordt geopend boven het AVG systeemvakpictogram (*mits u de standaardconfiguratie van het dialoogvenster* ***Geavanceerde instellingen/Weergave*** *ongewijzigd hebt gelaten)*.

Opmerking: *Bij tijdconflicten tussen een geplande programma-update en een geplande scan krijgt het updateproces een hogere prioriteit en zal het scannen worden onderbroken.*

10.11.3. Anti-Spam updateschema



Op het tabblad ***Taakinstellingen*** kunt u eerst het selectievakje ***Deze taak inschakelen*** uitschakelen als u de geplande ***Anti-Spam***-update tijdelijk niet wilt uitvoeren, en weer inschakelen als de noodzaak daarvoor zich aandient. Elementaire planning van ***Anti-Spam***-updates wordt beheerd met het onderdeel ***Updatebeheer***. In dat dialoogvenster kunt u gedetailleerd parameters instellen voor het updateschema. In het tekstveld ***Naam*** (*bij alle standaardschema's uitgeschakeld*) staat de naam die door de leverancier van het programma aan het schema is toegewezen.

Schema wordt uitgevoerd

geef een tijdsinterval op waarmee het nieuwe ***Anti-Spam***-updateschema moet worden uitgevoerd. U kunt deze 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 (***Actie bij het opstarten van de computer***).

Geavanceerde schemaopties

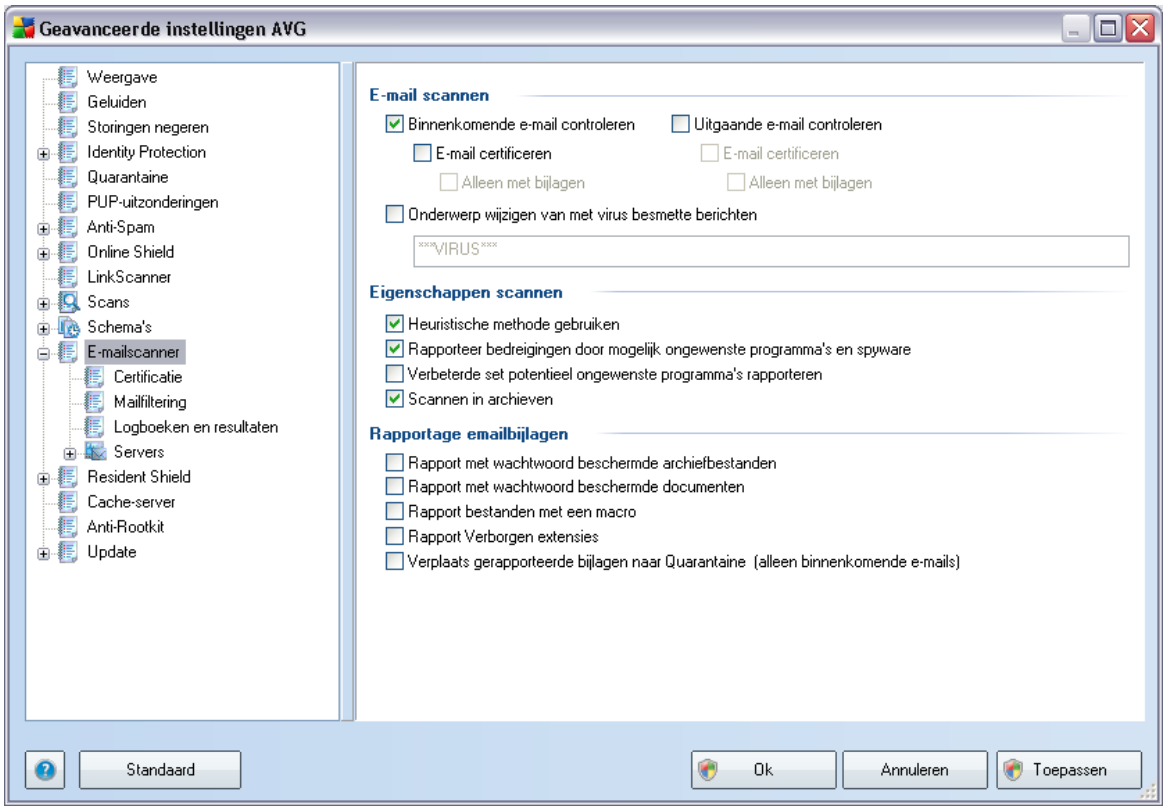
In deze sectie kunt u bepalen onder welke omstandigheden de ***Anti-Spam***-update wel of niet moet worden uitgevoerd als de computer in een energiebesparingsmodus is of helemaal is uitgeschakeld.

Overige update-instellingen

Schakel het selectievakje in bij ***Voer de update opnieuw uit zodra de internetverbinding beschikbaar is*** om ervoor te zorgen dat, als de internetverbinding verbroken wordt en de ***Anti-Spam***-updateprocedure mislukt, die onmiddellijk weer opnieuw zal worden uitgevoerd na herstel van de internetverbinding.

Zodra de geplande scan wordt gestart op de tijd die u hebt gespecificeerd, ontvangt u hierover een bericht via een pop-upvenster dat wordt geopend boven het AVG systeemladepictogram (*mits u de standaardconfiguratie van het dialoogvenster* ***Geavanceerde instellingen/Weergave*** *ongewijzigd hebt gelaten*.

10.12. E-mailscanner



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

- ***E-mail scannen*** – in het gedeelte kunt u het volgende instellen voor inkomende en uitgaande e-mailberichten:
    - Of de e-mailberichten moeten worden gescand op virussen.
    - Of een certificaat moet worden toegevoegd aan het einde van elk bericht met de melding dat het bericht geen virussen bevat. De tekst kan worden aangepast in het dialoogvenster Certificatie.
    - Of een certificaat alleen moet worden toegevoegd aan berichten met een bijlage.

Wilt u ***het onderwerp wijzigen van met virus besmette berichten***, dan schakelt u het selectievakje in en typt u de gewenste tekst in het tekstveld. Die

tekst zal dan worden toegevoegd aan de onderwerpregel van elk geïnfecteerd e-mailbericht, zodat het bericht beter als zodanig kan worden herkend en kan worden gefilterd. De standaardtekst is ***VIRUS***, het is raadzaam die te handhaven.

- ***Scaneigenschappen*** – in dit gedeelte kunt u opgeven hoe e-mailberichten moeten worden gescand:
    - ***Heuristische methode gebruiken*** – schakel dit selectievakje in om gebruik te maken van de heuristische detectiemethode voor het scannen van e-mailberichten. Als deze optie aan staat, kunt u e-mailbijlagen niet alleen op extensie filteren, maar wordt ook de feitelijke inhoud van de bijlage in ogenschouw genomen. De filtering kan worden ingesteld in het dialoogvenster Mailfiltering.
    - ***Bedreigingen door mogelijk ongewenste programma's en spyware rapporteren*** – (*standaard ingeschakeld*): schakel dit selectievakje in om de ***Anti-Spyware***-engine te activeren en naar spyware en virussen te scannen. Spyware behoort tot een twijfelachtige categorie malware en vormt gewoonlijk een veiligheidsrisico, maar sommige van deze programma's kunnen ook met opzet worden geïnstalleerd. Het is raadzaam deze functie niet uit te schakelen, omdat het de bescherming van uw computer vergroot.
    - ***Uitgebreide sets van mogelijk ongewenste programma's rapporteren*** – als de vorige optie is geactiveerd, kunt u ook dit selectievakje inschakelen om uitgebreide pakketten van spyware te detecteren: programma's waar op zich niets aan mankeert als u ze direct van de fabrikant krijgt, maar die wel in een later stadium voor kwaadaardige praktijken kunnen worden misbruikt. 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.
    - ***Scannen in archieven*** – schakel het selectievakje in om de inhoud van archieven te scannen die aan e-mailberichten zijn gekoppeld als bijlage.
- ***Rapportage e-mailbijlagen*** - in dit gedeelte kunt u extra rapportages instellen omtrent potentieel gevaarlijke of verdachte bestanden. NB: Er zal geen waarschuwingsvenster worden weergegeven, er wordt alleen een certificeringstekst toegevoegd aan het eind van het e-mailbericht en alle dergelijke rapporten worden vermeld in het dialoogvenster E-mail Scanner-detectie:
    - ***Met een wachtwoord beveiligde archieven rapporteren –*** archieven

(zip, rar, enzovoort) die beveiligd zijn met een wachtwoord, kunnen niet op virussen worden gescand; vink het vakje aan om deze als potentieel gevaarlijk te rapporteren.

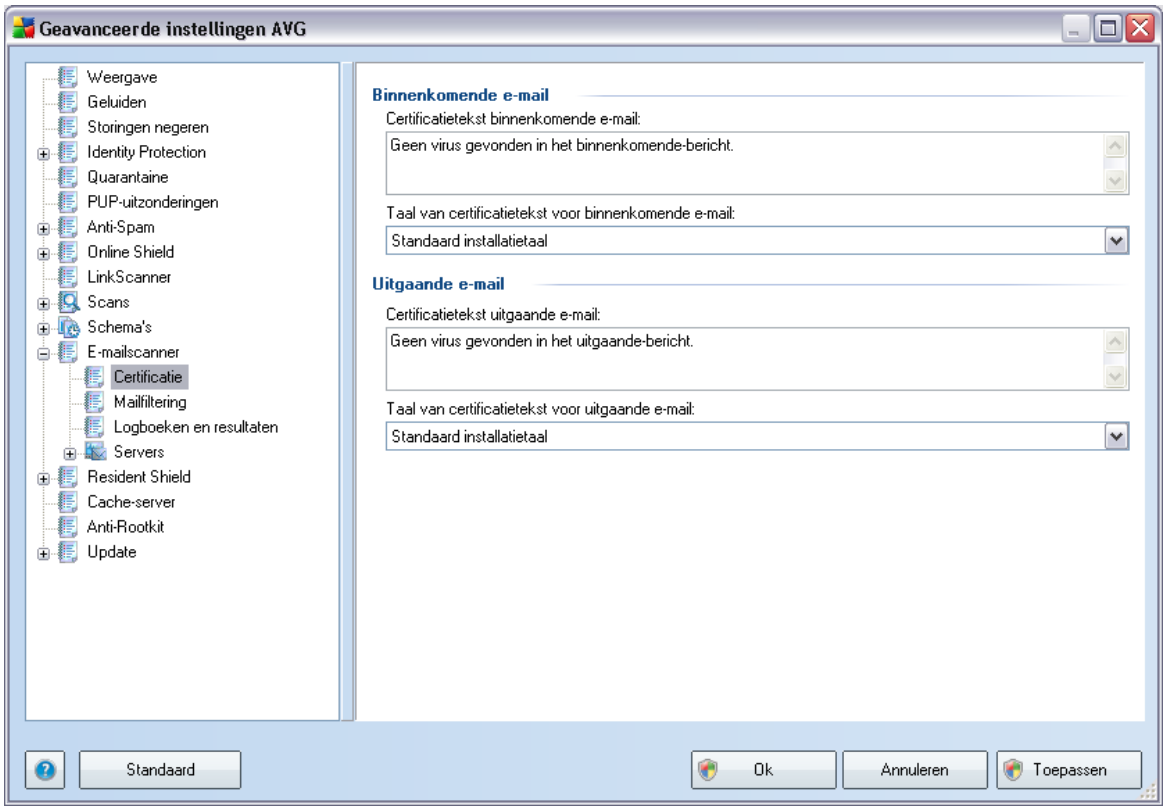
- ***Met een wachtwoord beveiligde documenten rapporteren*** – documenten die beveiligd zijn met een wachtwoord, kunnen niet op virussen worden gescand; schakel het selectievakje in om dergelijke documenten als potentieel gevaarlijk te rapporteren.

- ***Bestanden rapporteren die macro's bevatten*** – 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, en u wilt dit vak misschien aanvinken om ervoor te zorgen dat bestanden met macro's als verdacht worden gerapporteerd.

- ***Verborgen extensies rapporteren*** – dankzij een verborgen extensie ziet bijvoorbeeld een verdacht uitvoerbaar bestand "something.txt.exe" eruit als een onschuldig tekstbestand "something.txt".; schakel het selectievakje in om dergelijke bestanden als potentieel gevaarlijk te rapporteren.

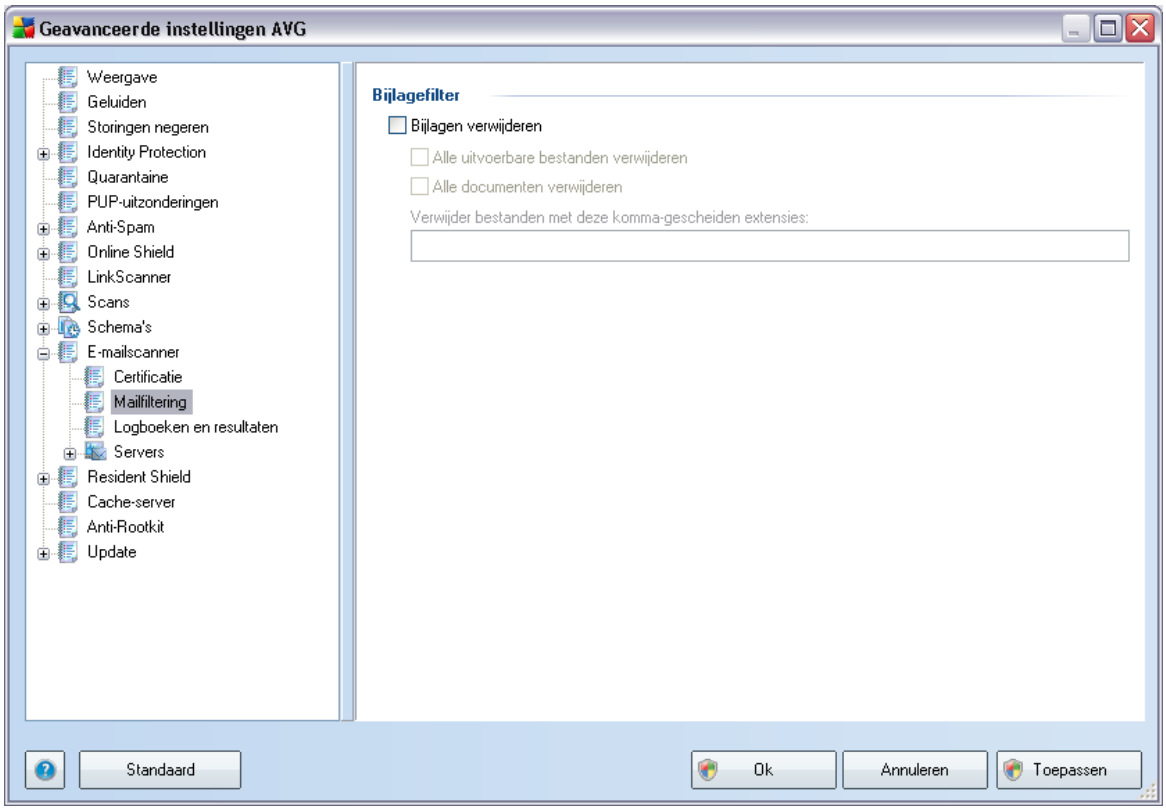
- ***Verplaats gerapporteerde bijlagen naar Quarantaine –*** geef op of u via e-mail op de hoogte wilt worden gesteld van de detectie van met een wachtwoord beveiligde archieven, met een wachtwoord beveiligde documenten, bestanden die macro's bevatten en/of bestanden met verborgen extensies die als bijlagen 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***.

10.12.1. Certificatie



In het dialoogvenster ***Certificatie*** kunt u precies opgeven wat moet worden weergegeven in de certificatietekst, en in welke taal. U geeft dit afzonderlijk op voor ***binnenkomende e-mail*** en ***uitgaande e-mail***.

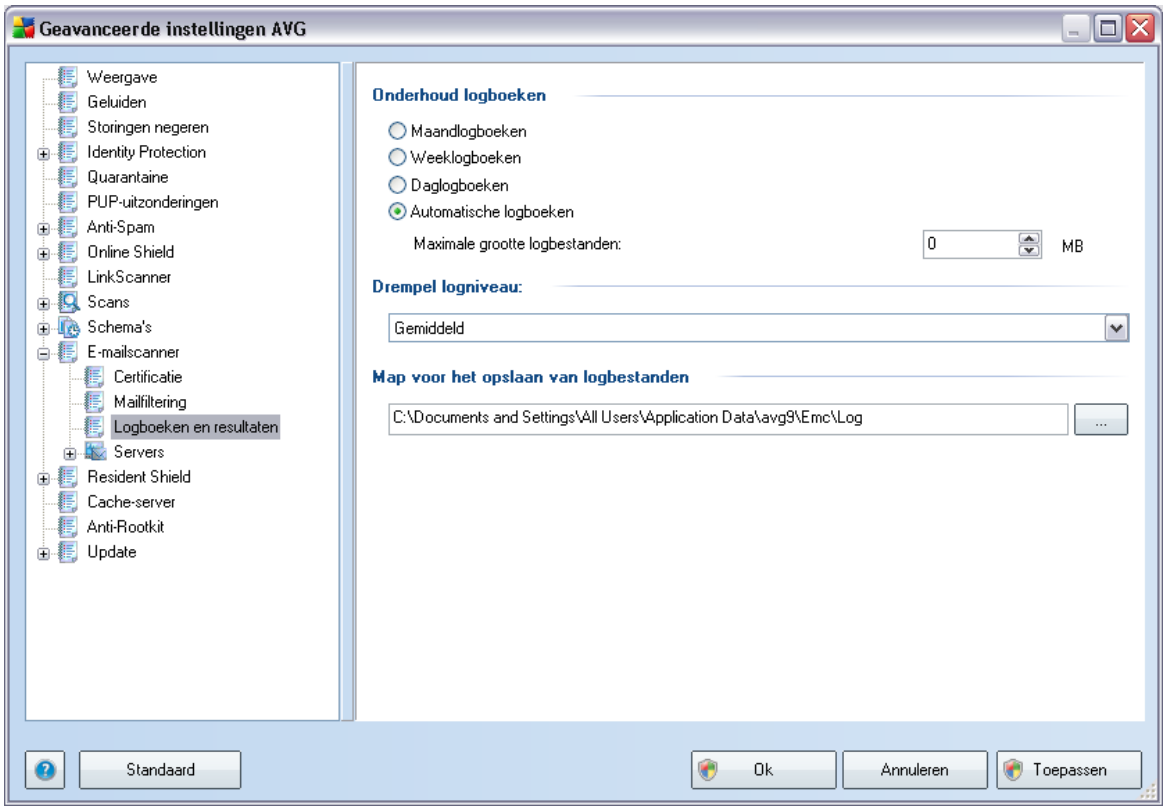
10.12.2. Mailfiltering



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 alle bijlagen bij e-mailberichten die worden herkend als geïnfecteerd of potentieel gevaarlijk, automatisch verwijderd. Als u wilt specificeren dat bepaalde typen bijlagen moeten worden verwijderd, schakelt u één 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

10.12.3. Logboeken en resultaten

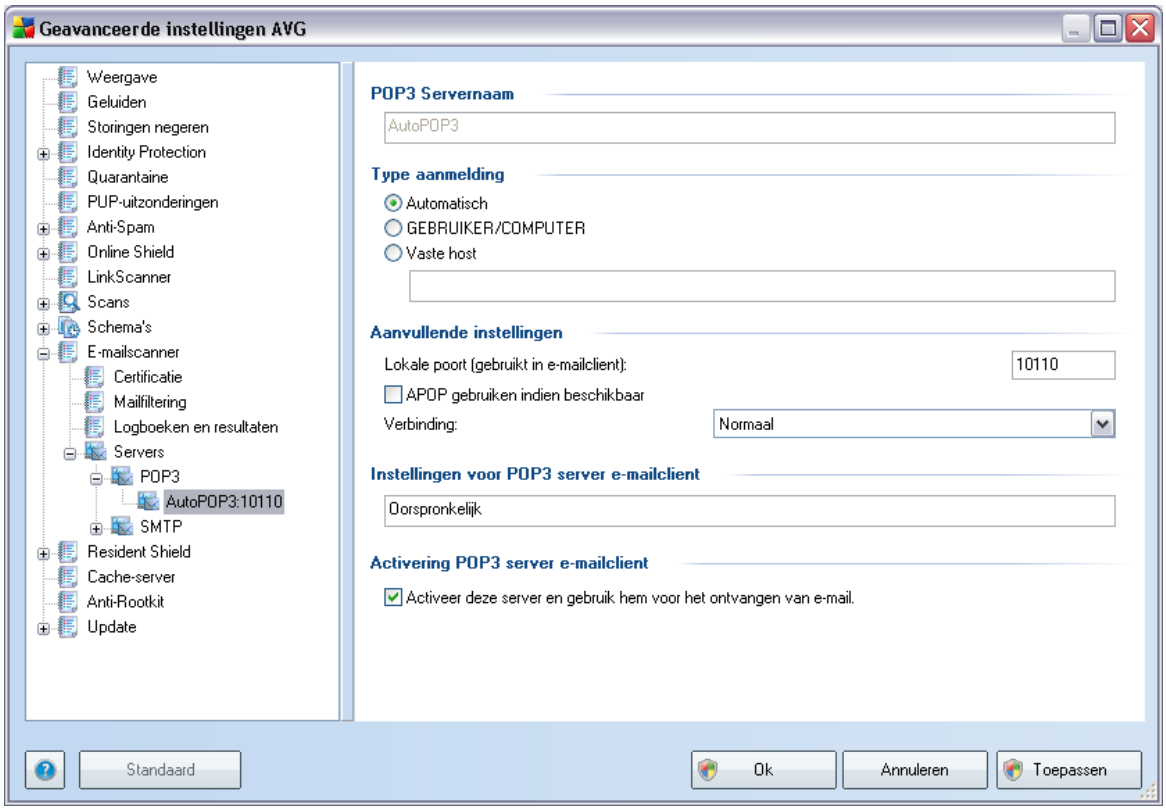


In het dialoogvenster dat u opent met de optie ***Logboeken en resultaten*** kunt u parameters opgeven voor het onderhoud van scanresultaten van e-mail. Het dialoogvenster is onderverdeeld in een aantal secties:

- ***Onderhoud logboeken*** - hier kunt u opgeven of u de gegevens van het scannen van e-mail dagelijks, wekelijks, maandelijks,... wilt opslaan, en bovendien hoe groot het logbestand maximaal mag zijn (*in MB*)
- ***Drempel logniveau*** - standaard is het gemiddelde niveau ingesteld - u kunt een lager niveau kiezen (*registreren van elementaire verbindingsinformatie*) of een hoger niveau (*registreren van al het verkeer*)
- ***Map voor het opslaan van logbestanden*** - hier kunt u de locatie van het logbestand opgeven

10.12.4. Servers

In het gedeelte ***Servers*** kunt u parameters wijzigen voor de servers van het onderdeel ***E-mailscanner*** of een nieuwe server installeren met de knop ***Nieuwe server toevoegen***.



In dit dialoogvenster (geopend met ***Servers / POP3***) kunt u een nieuwe ***E-mailscanner***-server instellen die gebruikmaakt van het POP3-protocol voor binnenkomende e-mail:

- ***POP3-servernaam*** - Typ de naam van de server of handhaaf de standaardnaam AutoPOP3
- ***Type aanmelding*** - bepaalt de methode voor het vaststellen van de mailserver die wordt gebruikt voor binnenkomende e-mailberichten:
    - ***Automatisch*** - Aanmelding wordt automatisch uitgevoerd, afhankelijk

van uw e-mailclientinstellingen.

- ***GEBRUIKER/COMPUTER*** - de eenvoudigste en meest gebruikte wijze om de doelmailserver te bepalen is de proxymethode. U gebruikt deze methode door de naam of het adres (of ook de poort) op te geven als deel van de aanmeldingsnaam van de gebruiker voor de specifieke mailserver. U scheidt de gegevens met het teken /. Zo gebruikt u user1/ pop.acme.com:8200 voor de aanmeldingsnaam voor de account user1 op de server pop.acme.com en de poort 8200.

- ***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-standaard poort 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*** - Meer gedetailleerde parameters opgeven:

  - ***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.

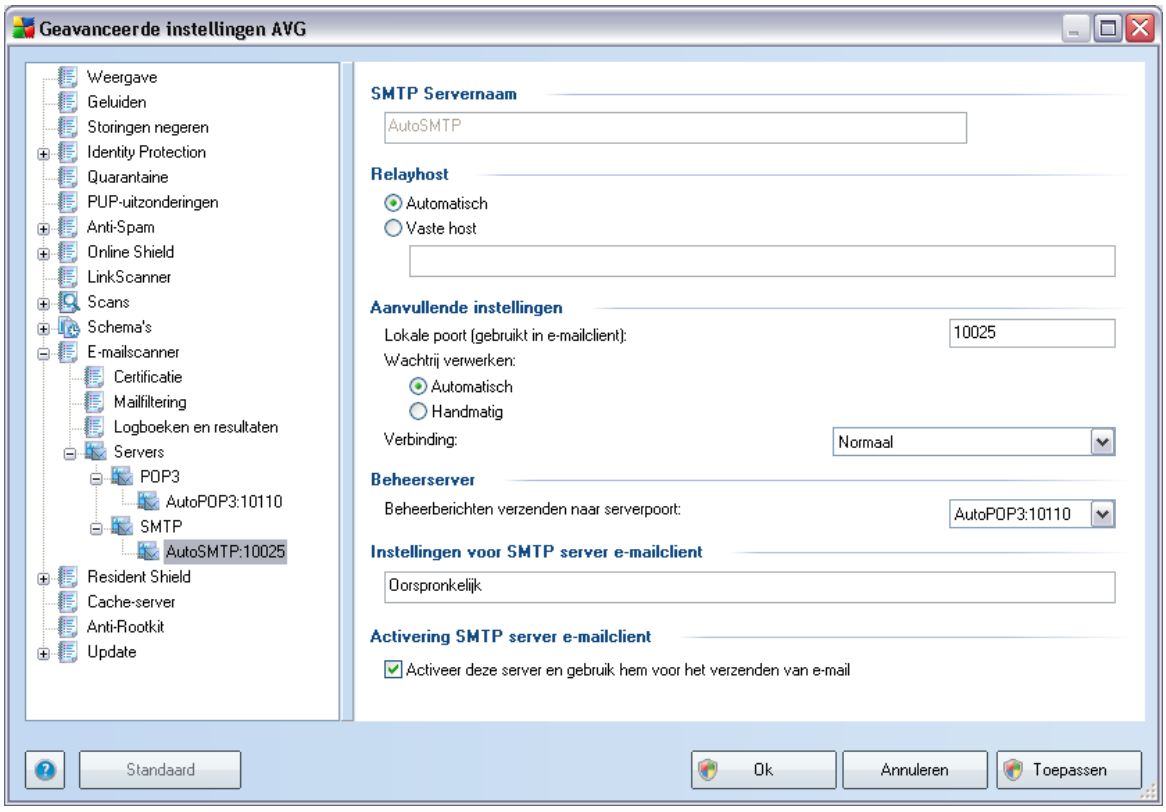
  - ***APOP gebruiken indien beschikbaar*** - deze optie biedt een veiligere e-mailserver aanmelding. Zo zorgt u ervoor dat de ***E-mailscanner*** een andere methode gebruikt om het accountwachtwoord van de gebruiker voor de aanmelding door te sturen. Het wachtwoord wordt dan niet in een open maar een gecodeerde indeling naar de server verstuurd met behulp van een variabelenketen die van de server ontvangen is. Deze functie is uiteraard alleen beschikbaar wanneer de doelmailserver de functie ondersteunt.

  - ***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.

- ***Instellingen voor POP3-server e-mailclient*** - hier staat beknopte informatie over de configuratie-instellingen die vereist zijn om uw e-mailclient goed te configureren (zodat de ***E-mailscanner*** alle binnenkomende e-mailberichten controleert). Dit is een overzicht dat is gebaseerd op de overeenkomende

parameters die in dit dialoogvenster en andere verwante dialoogvensters zijn opgegeven.

- ***Activering POP3 server e-mailclient*** - schakel dit selectievakje in of uit om de opgegeven POP3-server in of uit te schakelen



In dit dialoogvenster (geopend met ***Servers / SMTP***) kunt u een nieuwe ***E-mailscanner instellen*** server die gebruikmaakt van het SMTP-protocol voor uitgaande e-mail:

- ***SMTP-servernaam*** - Typ de naam van de server of handhaaf de standaardnaam AutoSMTP

- ***Hostrelay*** - Hiermee wordt de methode gedefinieerd voor het bepalen welke mailserver wordt gebruikt voor uitgaande e-mail:

    - ***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), evenals 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*** - Meer gedetailleerde parameters opgeven:

  - ***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.

  - ***Wachtrij verwerken*** - bepalen wat de ***E-mailscanner*** moet doen als de eisen voor het verzenden van e-mail worden verwerkt:

    - Automatisch - uitgaande e-mail wordt direct verzonden naar de doelmailserver

    - Handmatig - het bericht wordt in de wachtrij voor uitgaande berichten geplaatst en later verzonden

  - ***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.

- ***Beheerserver*** - weergave van het nummer van de poort van de server die gebruikt wordt voor de omgekeerde levering van beheerrapporten. Deze berichten worden bijvoorbeeld gegenereerd wanneer de doelmailserver het uitgaande bericht afwijst of wanneer deze mailserver niet beschikbaar is.

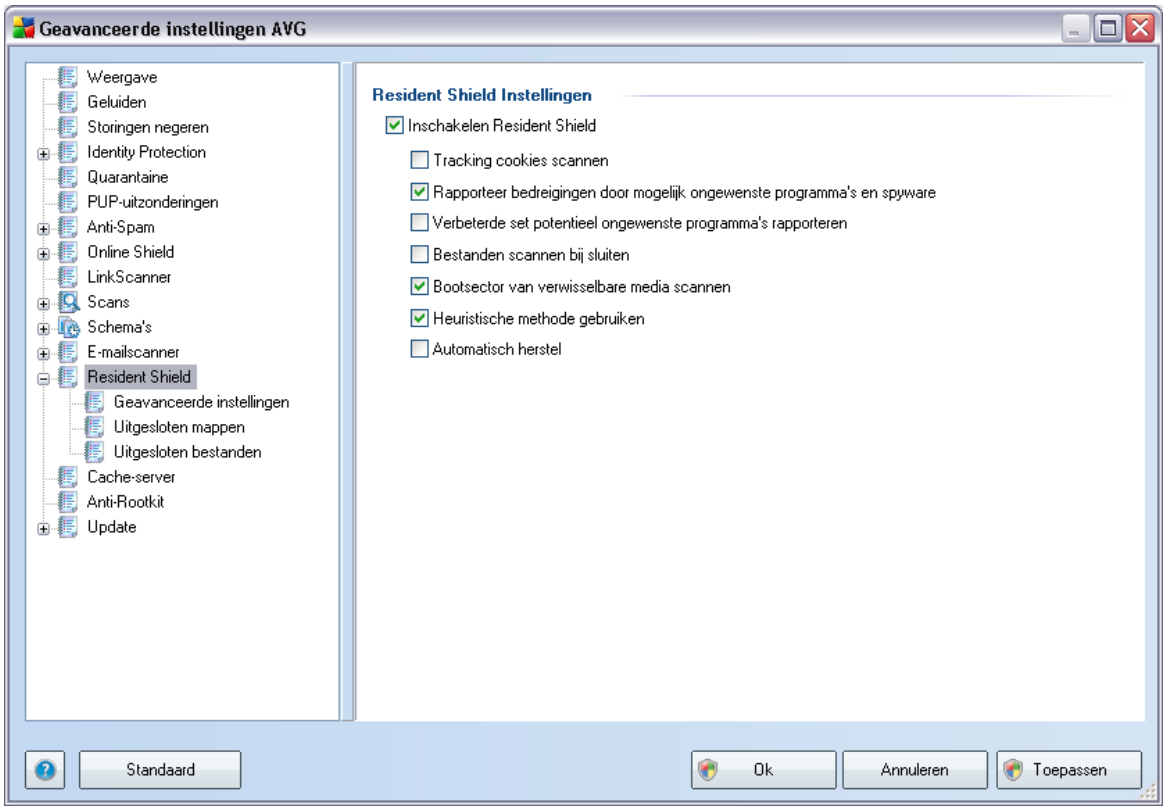
- ***Instellingen voor SMTP-server e-mailclient*** - korte instructies voor de configuratie van de clientmailtoepassing. De uitgaande e-mailberichten worden dan gecontroleerd met behulp van de server met de meest recente instellingen voor het controleren van uitgaande e-mailberichten. Dit is een overzicht dat is gebaseerd op de overeenkomende parameters die in dit dialoogvenster en andere verwante dialoogvensters zijn opgegeven.

- ***E-mailclient SMTP serveractivering*** - Schakel dit selectievakje in/uit om de

genoemde SMTP-server te activeren/deactiveren

10.13. Resident Shield

Het onderdeel ***Resident Shield*** voert live bescherming uit voor bestanden en mappen tegen virussen, spyware en andere malware.



In het dialoogvenster ***Instellingen Resident Shield*** kunt u de bescherming door ***Resident Shield*** volledig in- en uitschakelen met het selectievakje ***Resident Shield inschakelen*** (*deze optie is standaard ingeschakeld*). Bovendien kunt u instellen welke functies van ***Resident Shield*** moeten worden geactiveerd:

- ***Tracking cookies scannen*** - deze parameter geeft aan of u cookies wilt opsporen tijdens het scannen. (*HTTP-cookies worden gebruikt voor verificatie, tracking en het bijhouden van bepaalde informatie over gebruikers, bijvoorbeeld voorkeuren voor websites of de inhoud van winkelkarretjes*)
- ***Bedreigingen door mogelijk ongewenste programma's en spyware rapporteren*** - (*standaard ingeschakeld*): schakel dit selectievakje in om de

Anti-Spyware-engine te activeren en naar spyware en virussen te scannen. Spyware behoort tot een twijfelachtige categorie malware en vormt gewoonlijk een veiligheidsrisico, maar sommige van deze programma's kunnen ook met opzet worden geïnstalleerd. Het is raadzaam deze functie niet uit te schakelen, omdat het de bescherming van uw computer vergroot.

- ***Uitgebreide sets van mogelijk ongewenste programma's rapporteren*** - als de vorige optie is geactiveerd, kunt u ook dit selectievakje inschakelen om uitgebreide pakketten van spyware te detecteren: programma's waar op zich niets aan mankeert als u ze direct van de fabrikant krijgt, maar die wel in een later stadium voor kwaadaardige praktijken kunnen worden misbruikt. 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*** – Scannen bij afsluiten zorgt ervoor dat actieve objecten (bijv. toepassingen, documenten, enz.) worden gescand als ze worden geopend en gesloten; de functie levert een bijdrage aan de bescherming tegen bepaalde geavanceerde virustypen

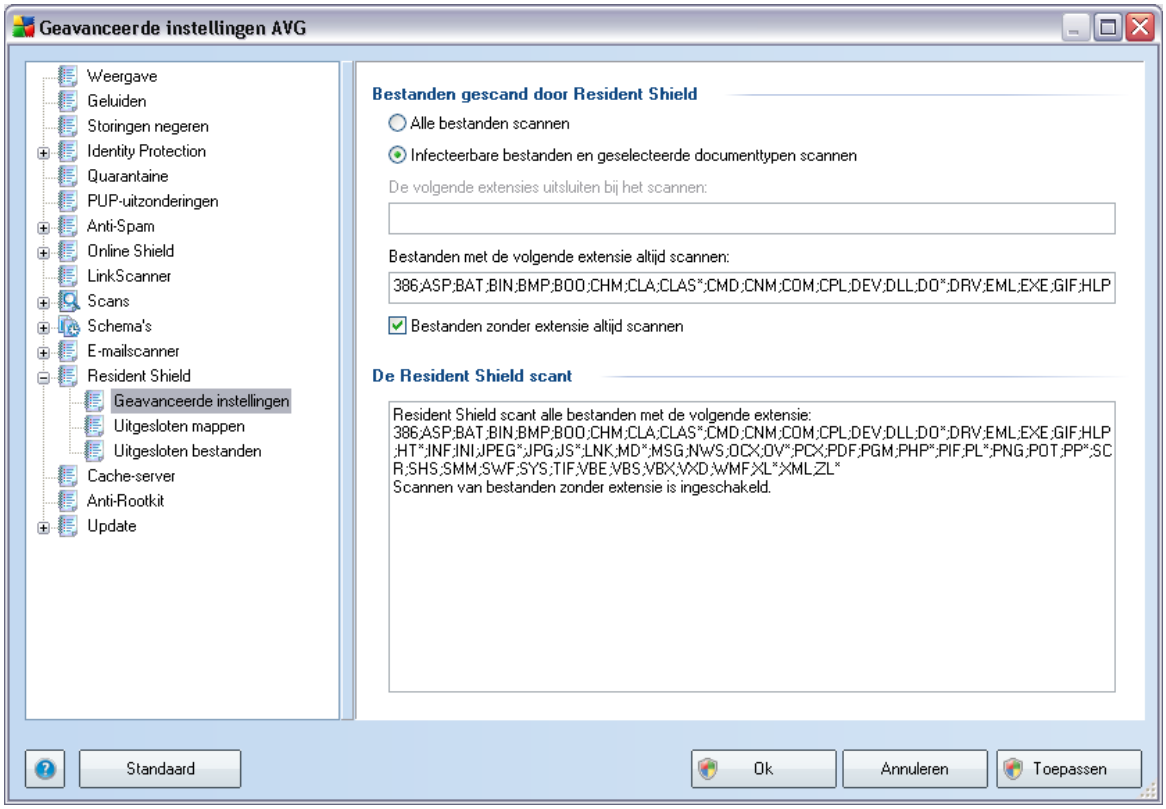
- ***Bootsector van verwisselbare media scannen*** – (*standaard ingeschakeld*)

- ***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

- ***Automatisch herstel*** – gedetecteerde infecties worden automatisch hersteld als er een remedie beschikbaar is

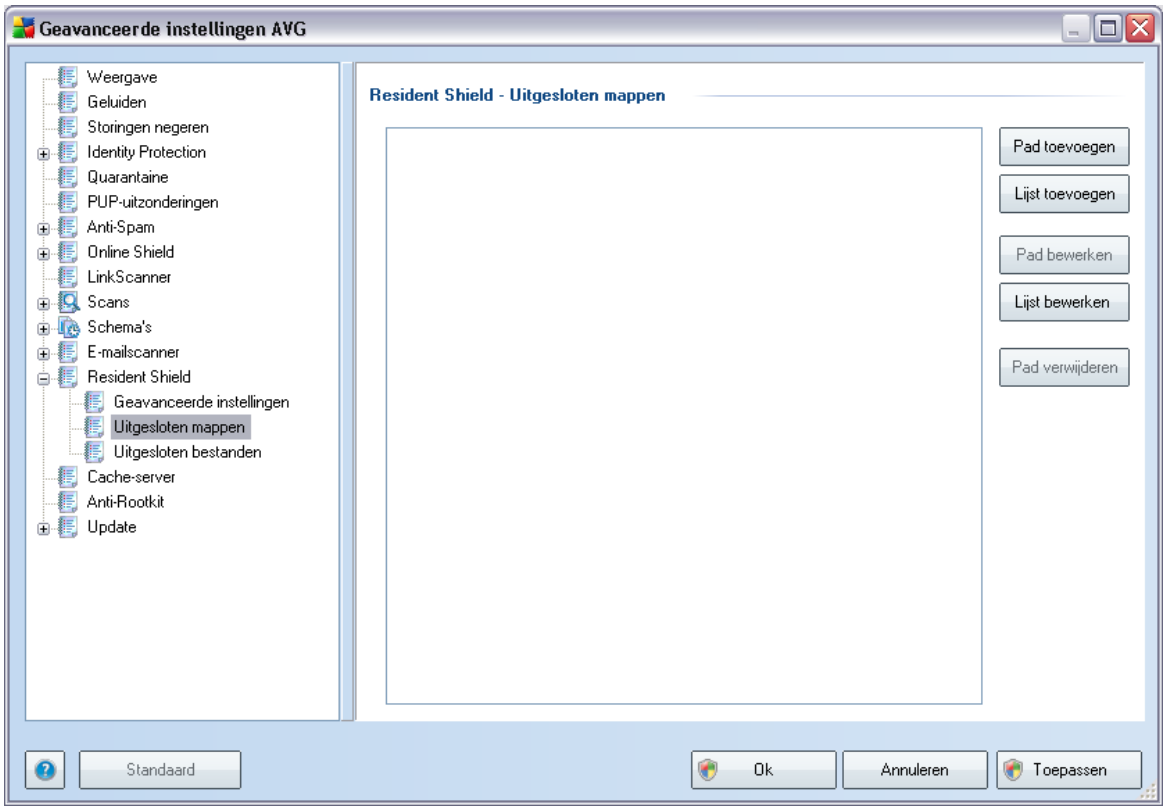
10.13.1. Geavanceerde instellingen

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



Maak een keuze of u alle bestanden wilt scannen of alleen infecteerbare bestanden - in dat laatste geval kunt u een lijst opgeven met extensies van bestanden die moeten worden genegeerd bij het scannen, en een lijst met extensies van bestanden die onder alle omstandigheden moeten worden gescand.

10.13.2. Uitgesloten mappen



In het dialoogvenster ***Uitsluitingen voor directory met Resident Shield*** kunt u mappen opgeven die ***Resident Shield*** moet negeren.

Het wordt met klem aangeraden om geen mappen over te slaan, tenzij dit absoluut noodzakelijk is!

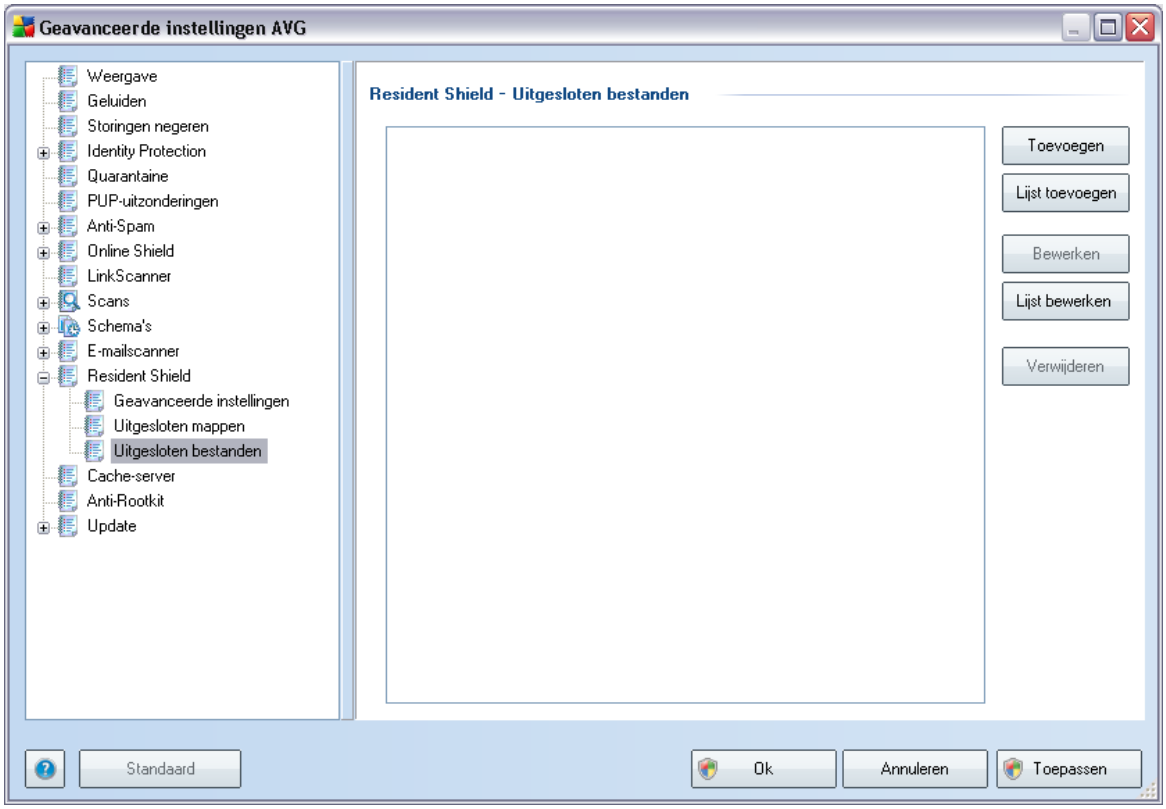
Dit dialoogvenster heeft de volgende knoppen:

- ***Pad toevoegen***– klik op deze knop om mappen op te geven die tijdens het scannen moeten worden overgeslagen. U kunt deze mappen vervolgens één voor één selecteren in de navigatiestructuur van de lokale schijf
- ***Lijst toevoegen***– klik op deze knop als u een hele lijst met mappen wilt toevoegen die tijdens het scannen door ***Resident Shield*** moeten worden overgeslagen
- ***Pad bewerken***– klik op deze knop als u het opgegeven pad naar een

geselecteerde map wilt bewerken

- ***Lijst bewerken***– klik op deze knop om de lijst met mappen te bewerken
- ***Pad verwijderen***– klik op deze knop om het pad naar een geselecteerde map uit de lijst te verwijderen

10.13.3. Uitgesloten bestanden



Het dialoogvenster ***Resident Shield - Uitgesloten bestanden*** werkt net zo als het eerder besproken ***Resident Shield - Uitgesloten mappen***, maar in dit dialoogvenster kunt u bestanden opgeven die niet door ***Resident Shield*** moeten worden gescand.

Het wordt met klem aangeraden om geen bestanden over te slaan, tenzij dit absoluut noodzakelijk is!

Dit dialoogvenster heeft de volgende knoppen:

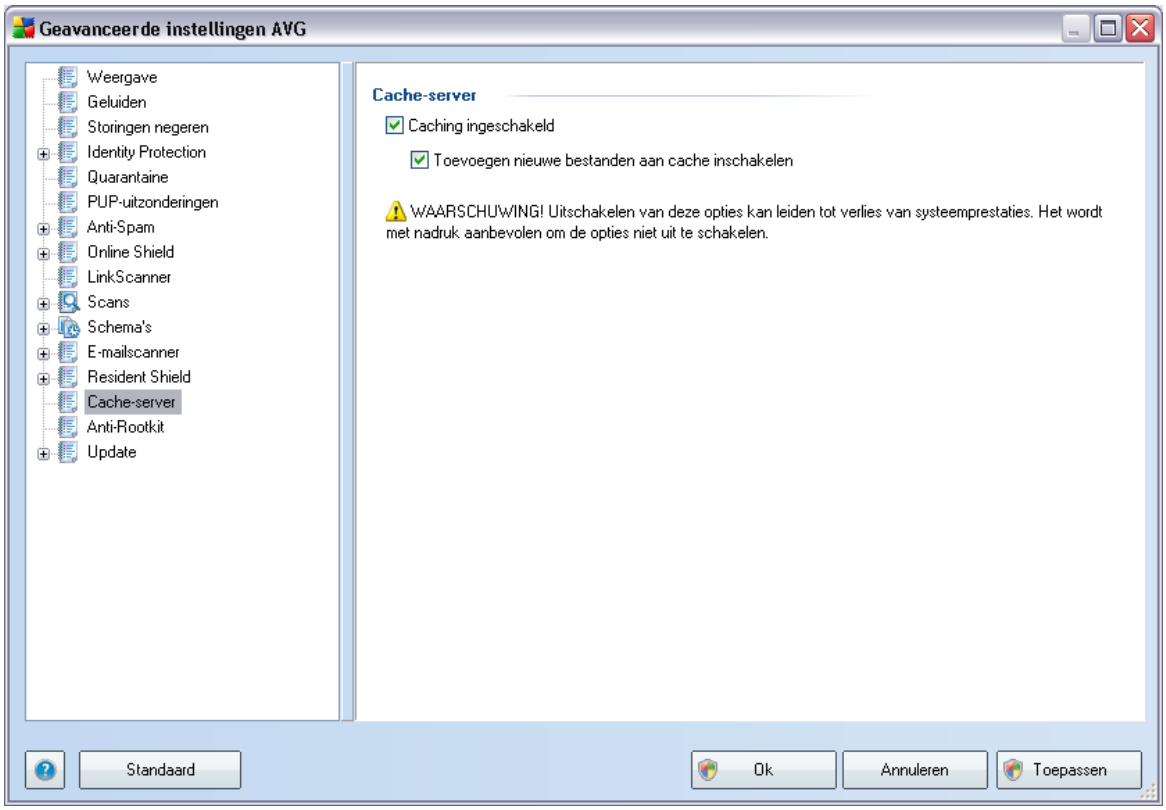
- ***Toevoegen*** – klik op deze knop om bestanden op te geven die tijdens het

scannen moeten worden overgeslagen. U kunt deze mappen vervolgens één voor één selecteren in de navigatiestructuur van de lokale schijf

- ***Lijst toevoegen*** – klik op deze knop als u een complete lijst met bestanden wilt toevoegen die tijdens het scannen door ***Resident Shield*** moeten worden overgeslagen
- ***Bewerken*** – klik op deze knop als u het opgegeven pad naar een geselecteerd bestand wilt bewerken
- ***Lijst bewerken*** – klik op deze knop om de lijst met bestanden te bewerken
- ***Verwijderen*** – klik op deze knop om het pad naar een geselecteerd bestand uit de lijst te verwijderen

10.14. Cache-server

De***Cache-server*** is een proces dat is ontwikkeld om scans te versnellen (*scans op verzoek, geplande scans van de hele computer, scans door Resident Shield).* De Cache-server verzamelt informatie over vertrouwde bestanden (*bijvoorbeeld bestanden met een digitale handtekening*): die bestanden worden vervolgens als veilig beschouwd en bij het scannen overgeslagen.



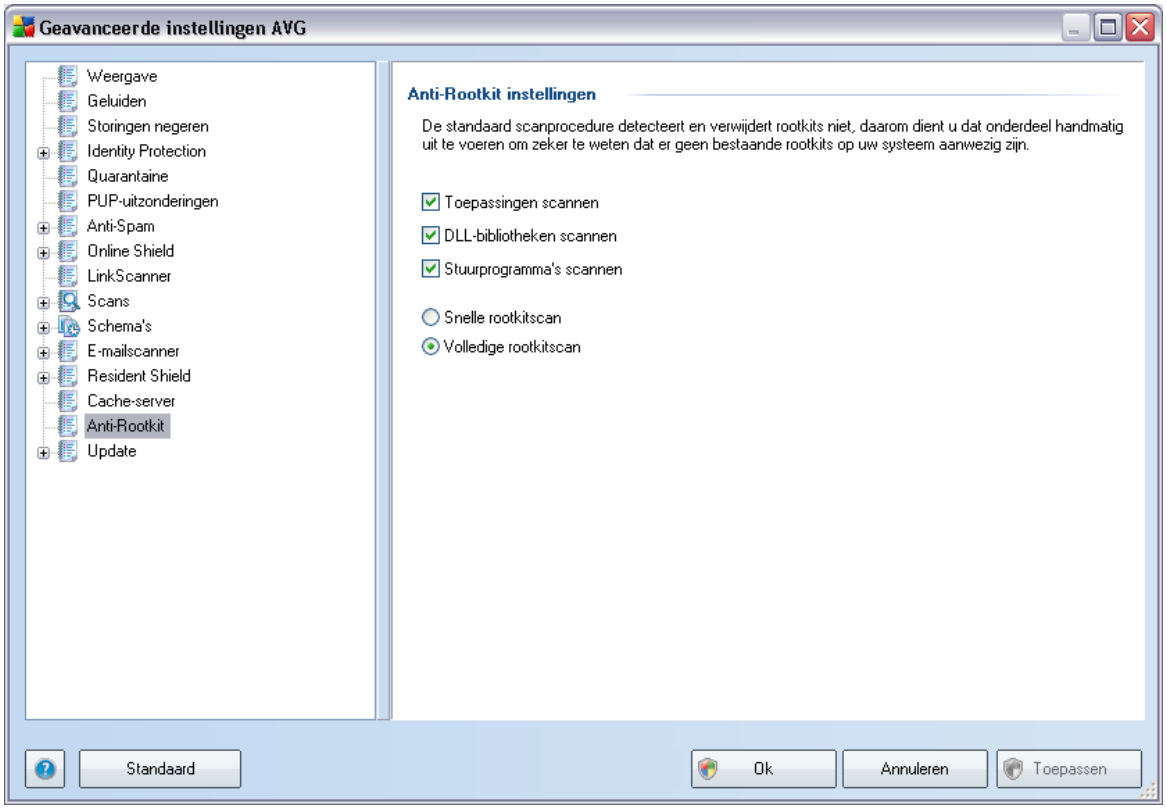
In dit dialoogvenster kunt u uit twee instellingen kiezen:

- ***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.

10.15. Anti-Rootkit

In dit dialoogvenster kunt u de configuratie van het onderdeel ***Anti-rootkit*** bewerken:



Bewerking van alle functies van de ***Anti-rootkit***zoals deze worden aangeboden in dit dialoogvenster is ook rechtstreeks toegankelijk vanuit de ***interface van het onderdeel Anti-rootkit***.

Schakel de selectievakjes in van de objecten die moeten worden gescand:

- ***Toepassingen scannen***
- ***DLL-bibliotheken scannen***
- ***Stuurprogramma's scannen***

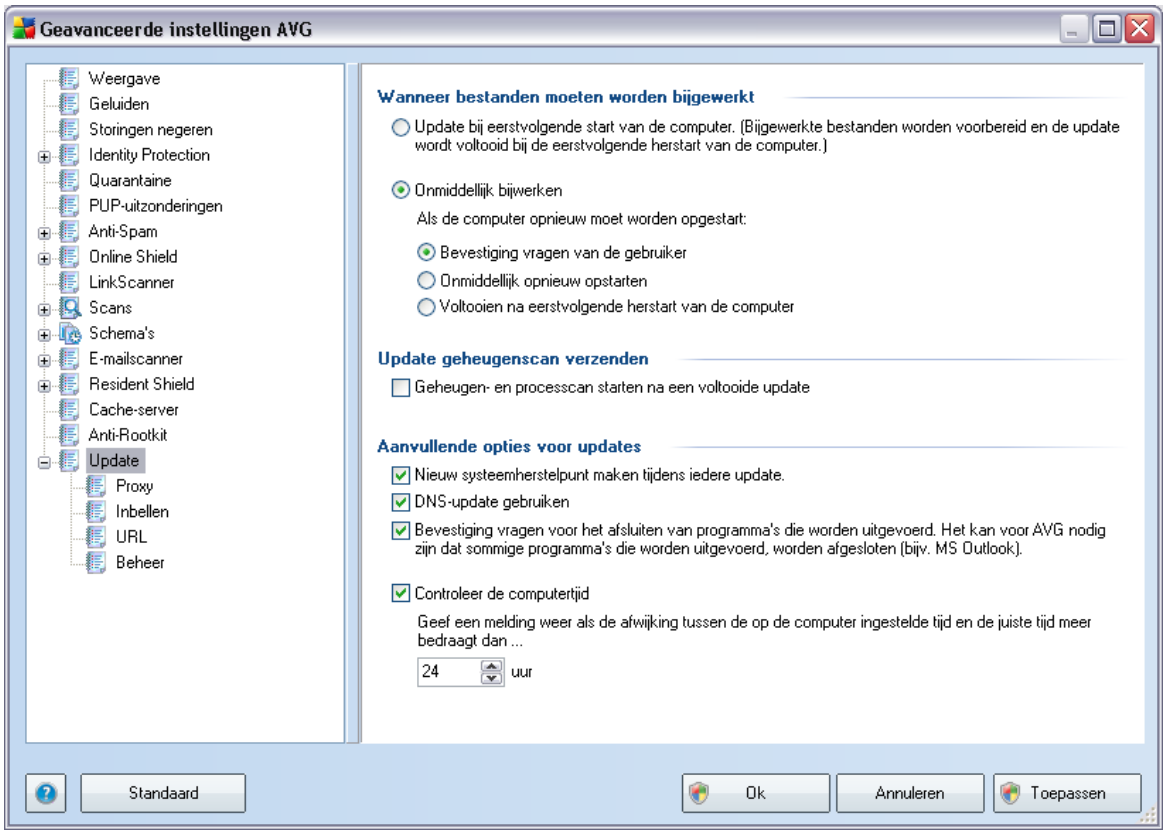
Vervolgens kunt u de scanmodus kiezen:

- ***Snelle rootkitscan*** - scant 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*)

10.16. Update



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 kiezen uit twee mogelijkheden: u kunt een update plannen voor de eerstvolgende start van de pc, of de update meteen uitvoeren. Standaard is de optie voor onmiddellijk uitvoeren van een update ingesteld, omdat AVG op die manier een maximaal beveiligingsniveau kan bereiken. Plannen van een update voor de

eerstvolgende keer dat de pc wordt opgestart is alleen raadzaam als u zeker weet dat de computer regelmatig opnieuw wordt opgestart, minstens één keer per dag.

Als u besluit de standaardconfiguratie aan te houden en de updateprocedure meteen uit te voeren, kunt u opgeven onder welke omstandigheden een eventueel vereiste herstart van de computer moet worden uitgevoerd:

- ***Bevestiging vragen van de gebruiker*** - u wordt gevraagd een herstart te bevestigen die nodig is voor het voltooien van de updateprocedure.
- ***Onmiddellijk opnieuw opstarten*** - de computer wordt automatisch opnieuw gestart nadat de updateprocedure is voltooid, u hoeft daarvoor geen toestemming meer te verlenen
- ***Voltooien na opstarten van de computer*** - de updateprocedure wordt pas voltooid als de computer opnieuw wordt opgestart - houd ook hierbij in het oog dat deze optie alleen raadzaam is als u zeker weet dat de computer regelmatig opnieuw wordt opgestart, minstens één keer per dag.

Update geheugenscan verzenden

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.

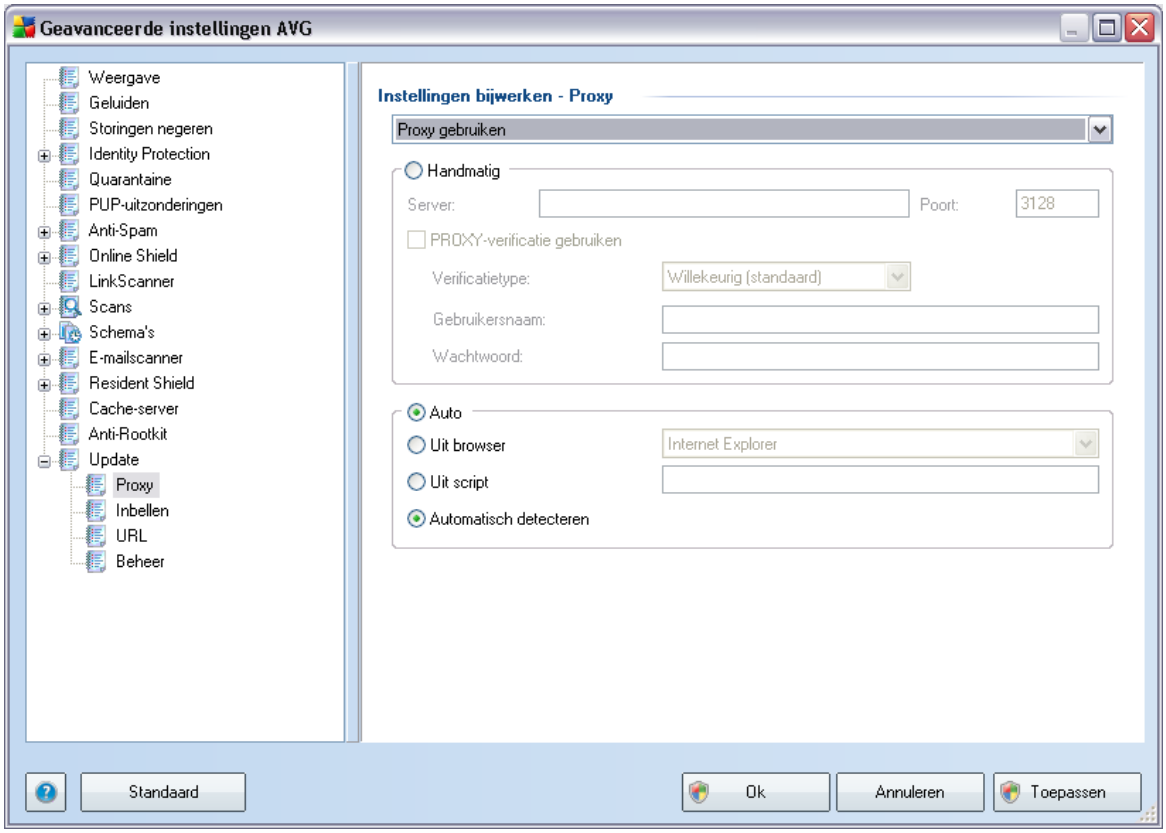
Aanvullende opties voor updates

- ***Nieuw systeemherstelpunt maken na iedere programma-update*** - er wordt een nieuw systeemherstelpunt gemaakt voor elke programma-update van AVG. Als de updateprocedure faalt en uw besturingssysteem crasht, kunt u uw besturingssysteem altijd herstellen in de oorspronkelijke configuratie vanaf dit punt. Deze optie is toegankelijk via Start / Alle programma's / Accessoires / Systeemprogramma's / Systeemherstel, maar het aanbrengen van wijzigingen wordt alleen aanbevolen aan ervaren gebruikers! Schakel dit selectievakje niet uit als u van deze functionaliteit wilt gebruikmaken.
- ***DNS-update gebruiken*** - schakel dit selectievakje in om te bevestigen dat u gebruik wilt maken van de detectiemethode voor updatebestanden die de hoeveelheid gegevens reduceert die wordt overgebracht van de updateserver naar de AVG-client;
- ***Bevestiging vragen om actieve toepassingen te sluiten*** (*standaard*

ingeschakeld) - deze optie zorgt ervoor dat u zeker weet dat er geen toepassingen die worden uitgevoerd, zullen worden afgesloten zonder uw expliciete toestemming - mocht dat afsluiten nodig zijn voor het voltooien van de updateprocedure;

- ***Controleer de computertijd*** - schakel deze optie in om aan te geven dat u er van op de hoogte wilt worden gesteld als de computertijd afwijkt van de juiste tijd met meer dan een opgegeven aantal uren.

10.16.1. 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 gebruiken***

- ***Proxyserver niet gebruiken*** – standaardinstelling
- ***Proberen te verbinden via proxy, en als dat niet lukt direct verbinden***

Als u een optie selecteert waarbij een proxyserver betrokken is, zult u aanvullende gegevens moeten verstrekken. 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*)

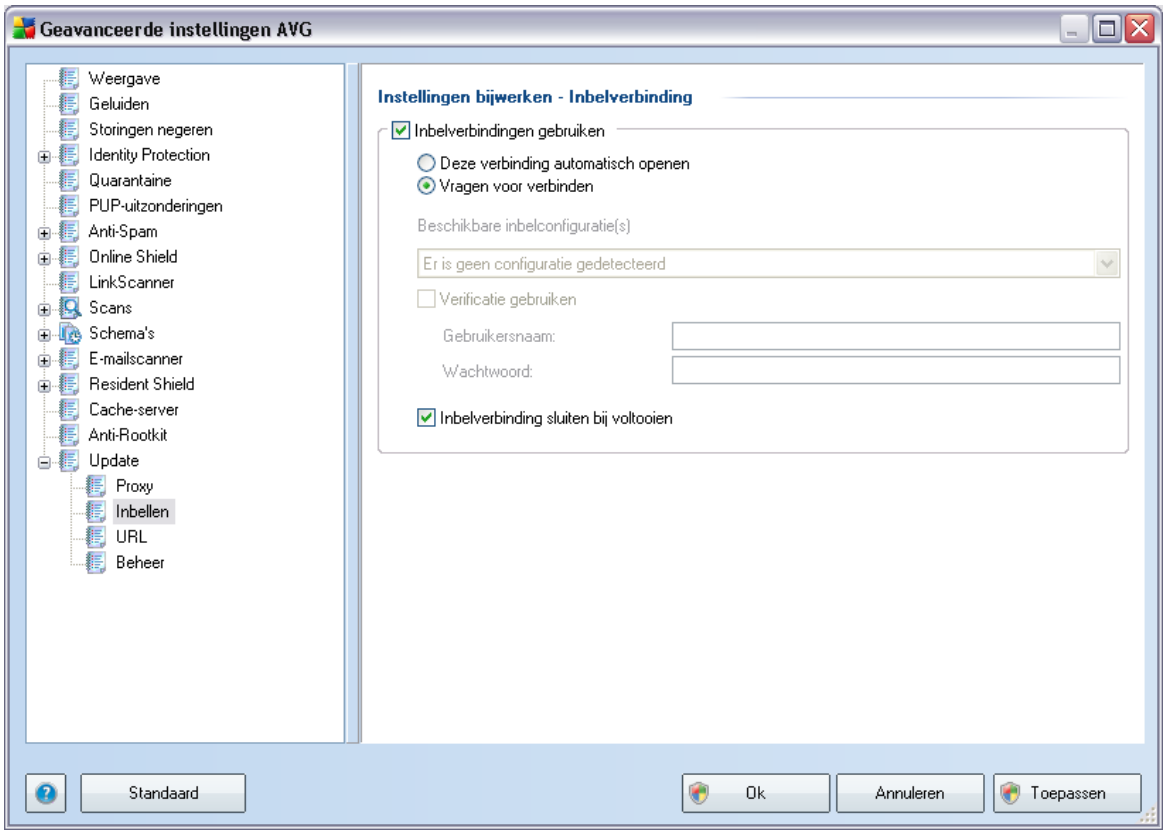
Het is mogelijk op de proxyserver voor de afzonderlijke gebruikers verschillende regels in te stellen. Als dat voor uw proxyserver het geval is, schakelt u het selectievakje ***PROXY-verificatie gebruiken*** in om te controleren of uw gebruikersnaam en wachtwoord geldig zijn voor een verbinding met internet 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 standaardbrowser voor internet
- ***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

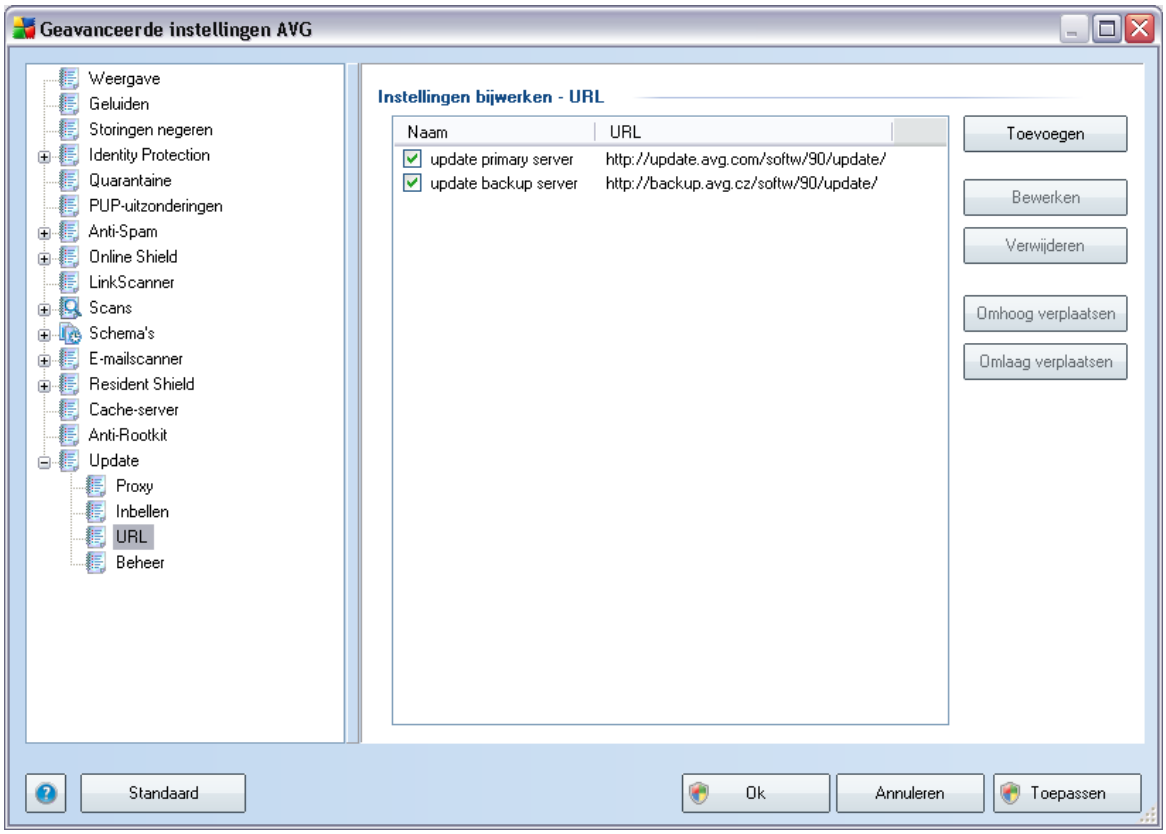
10.16.2. Inbellen



Alle parameters die optioneel zijn gedefinieerd in het dialoogvenster ***Instellingen bijwerken - Inbelverbinding*** hebben betrekking op een inbelverbinding met internet. De opties op het tabblad zijn uitgeschakeld, tenzij u het selectievakje ***Inbelverbindingen gebruiken*** inschakelt.

Stel in of u automatisch een verbinding met internet tot stand wilt brengen (***Deze verbinding automatisch openen***) of geef aan dat u de verbinding telkens handmatig tot stand wilt brengen (***Vragen om verbinding***). Bij een automatische verbinding moet u ook nog aangeven of de verbinding moet worden verbroken nadat de update is voltooid (***Inbelverbinding sluiten bij voltooien***).

10.16.3. URL



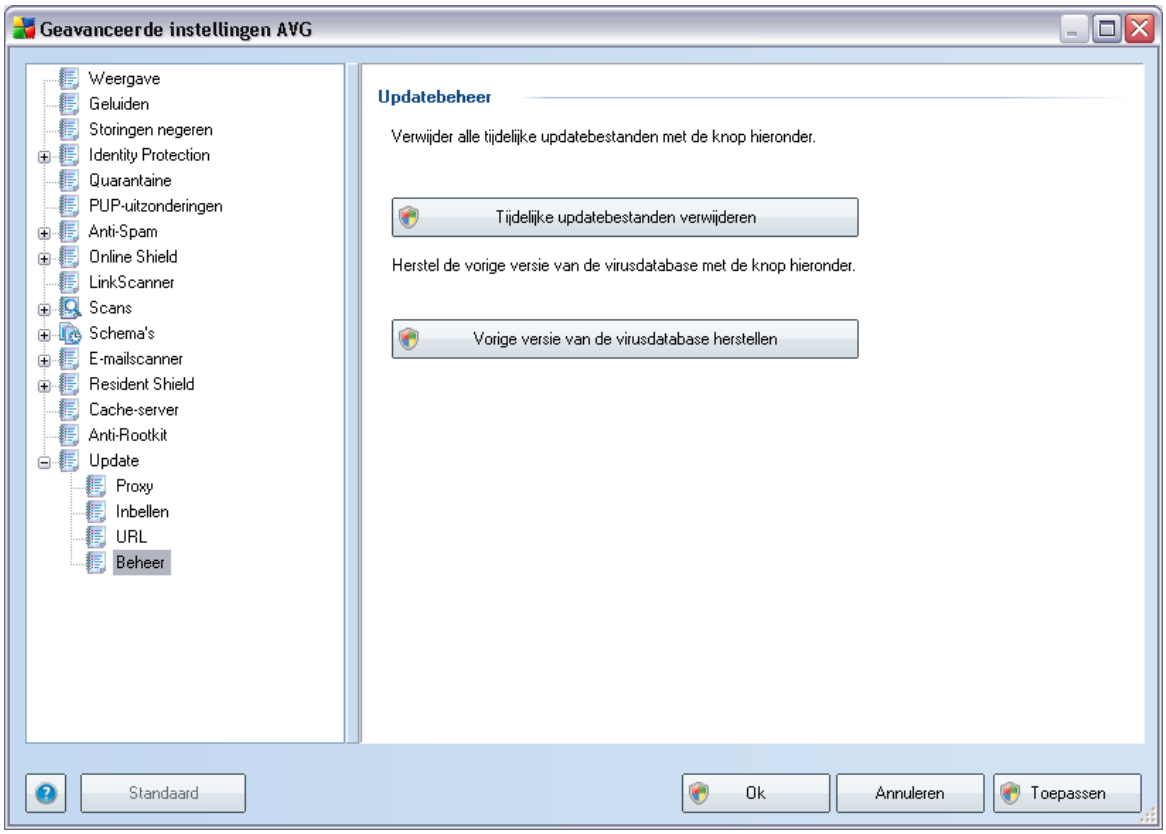
Op het tabblad ***URL*** wordt een lijst met internetadressen weergegeven die u kunt gebruiken om de updatebestanden te downloaden. De lijst en de vermeldingen kunnen worden gewijzigd met behulp van de volgende knoppen:

- ***Toevoegen***– als u op deze knop klikt, wordt er een dialoogvenster geopend waarin u een nieuwe URL kunt opgeven die aan de lijst moet worden toegevoegd
- ***Bewerken*** - als u op deze knop klikt, wordt er een dialoogvenster geopend waarin u de parameters van de geselecteerde URL kunt bewerken
- ***Verwijderen***– als u op deze knop klikt, wordt de geselecteerde URL uit de lijst verwijderd
- ***Omhoog verplaatsen***– als u op deze knop klikt, wordt de geselecteerde URL één positie hoger op de lijst geplaatst

- ***Omlaag verplaatsen*** - als u op deze knop klikt, wordt de geselecteerde URL één positie lager in de lijst geplaatst

10.16.4. Beheer

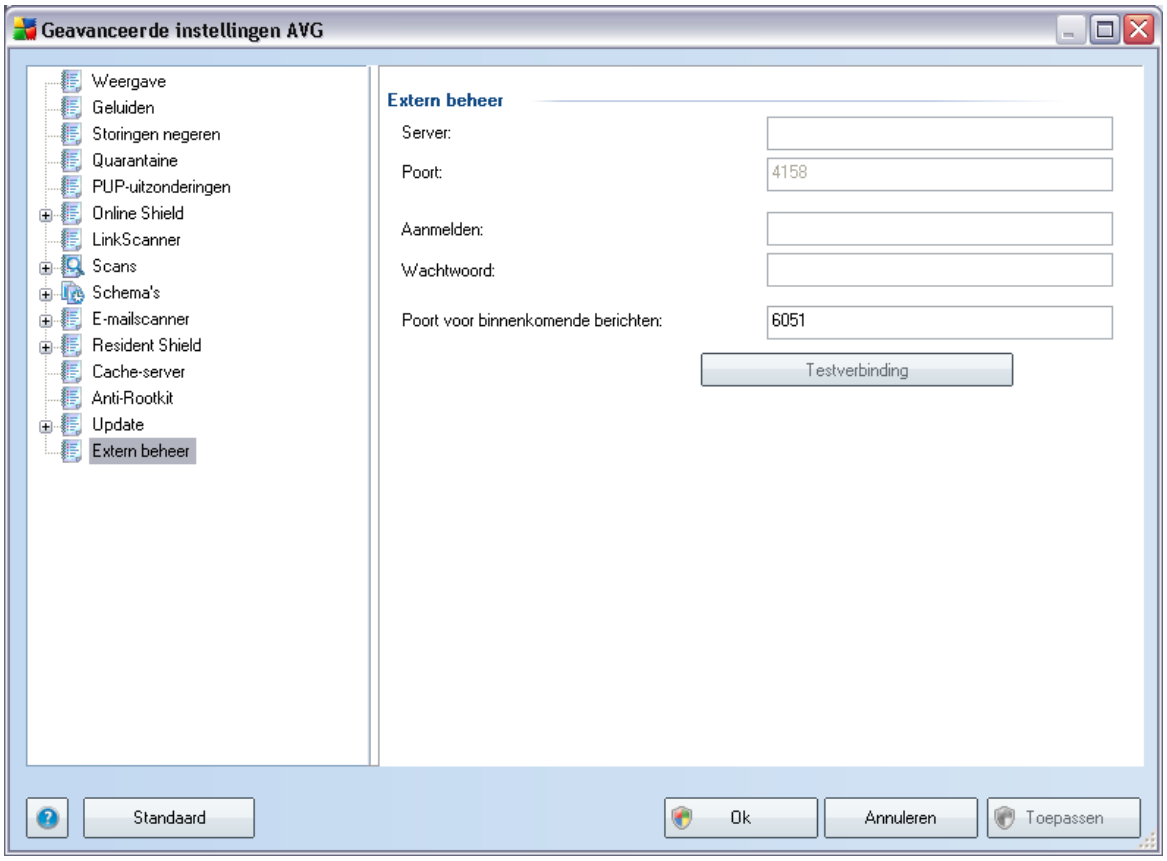
In het dialoogvenster ***Beheer*** staan twee knoppen voor opties:



- ***Tijdelijke bestanden verwijderen***- klik op deze knop als u alle redundante updatebestanden wilt verwijderen van uw vaste schijf (*standaard blijven deze bestanden 30 dagen opgeslagen*)

- ***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*)

10.17. Extern beheer



De instellingen voor ***Extern beheer*** hebben betrekking op de verbinding tussen het AVG clientstation en het systeem voor extern beheer. Als u van plan bent een verbinding tot stand te brengen tussen het desbetreffende station en extern beheer, geeft u de volgende parameters op:

- ***Server*** - de naam van de server (of het IP-adres van de server) waarop AVG Admin Server is geïnstalleerd
- ***Poort*** - geef het poortnummer op dat de AVG client gebruikt voor communicatie met AVG Admin Server(*het standaard poortnummer is 4158 - als dat poortnummer wordt weergegeven, hoeft u het niet expliciet te specificeren*)
- ***Aanmelden*** - Als de communicatie tussen de AVG client en AVG Admin Server wordt gedefinieerd als beveiligd, geeft u uw gebruikersnaam op ...

- ***Wachtwoord*** - ... en uw wachtwoord
- ***Poort voor binnenkomende berichten*** - het nummer van de poort waarlangs de AVG client binnenkomende berichten van AVG Admin Server accepteert

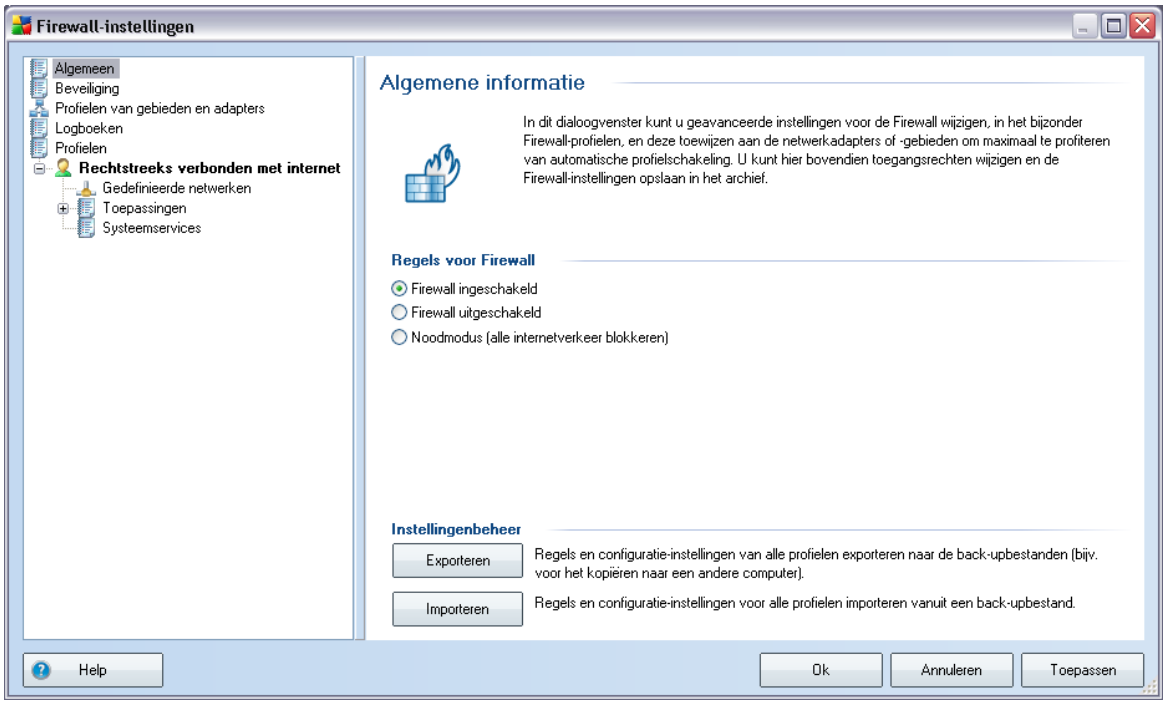
Met de knop ***Testverbinding*** kunt u controleren of alle hierboven weergegeven gegevens geldig zijn en er met succes een verbinding tot stand gebracht kan worden met DataCenter.

Opmerking:*Raadpleeg de documentatie van AVG Network Edition voor een uitgebreide beschrijving van extern beheer.*

11. Firewall-instellingen

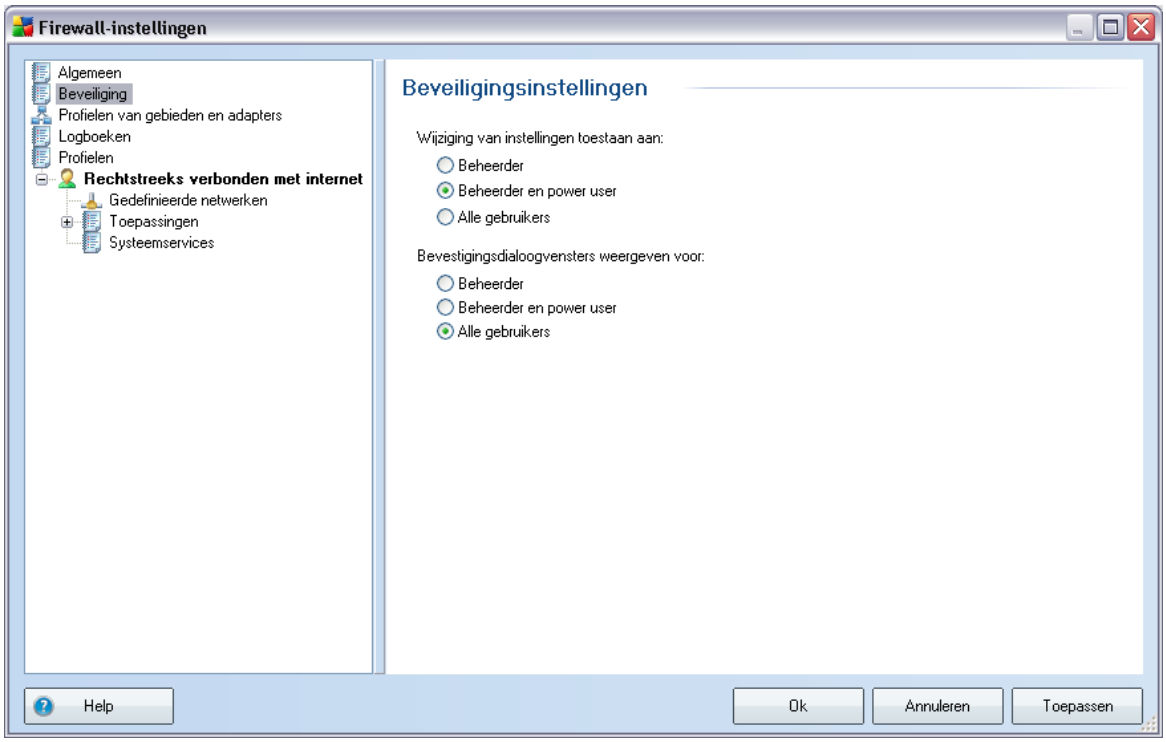
De configuratie van de ***Firewall*** wordt geopend in een nieuw venster van waaruit met behulp van diverse dialoogvensters geavanceerde parameters kunnen worden ingesteld voor het onderdeel. ***Geavanceerd bewerken van de configuratie is echter alleen bedoeld voor experts en ervaren gebruikers.***

11.1. Algemeen



In het gedeelte ***Algemene informatie*** kunt u een ***Firewall***-configuratie ***exporteren*** / ***importeren***; u exporteert bijvoorbeeld de gedefinieerde ***Firewall***-regels en instellingen naar de back-upbestanden of importeert het back-upbestand.

11.2. Beveiliging



In het dialoogvenster ***Beveiligingsinstellingen*** kunt u algemene regels opstellen voor de ***Firewall***, ongeacht het geselecteerde profiel:

- ***Wijzigingen toestaan door*** - specificeren wie de configuratie van de ***Firewall*** mag wijzigen
- ***Bevestiging vragen voor*** - specificeren aan wie de bevestigingsdialoogvensters (*dialoogvensters waarin een beslissing moet worden genomen in die gevallen die niet worden gedekt door een gedefinieerde* ***Firewall****-regel*) moeten worden getoond

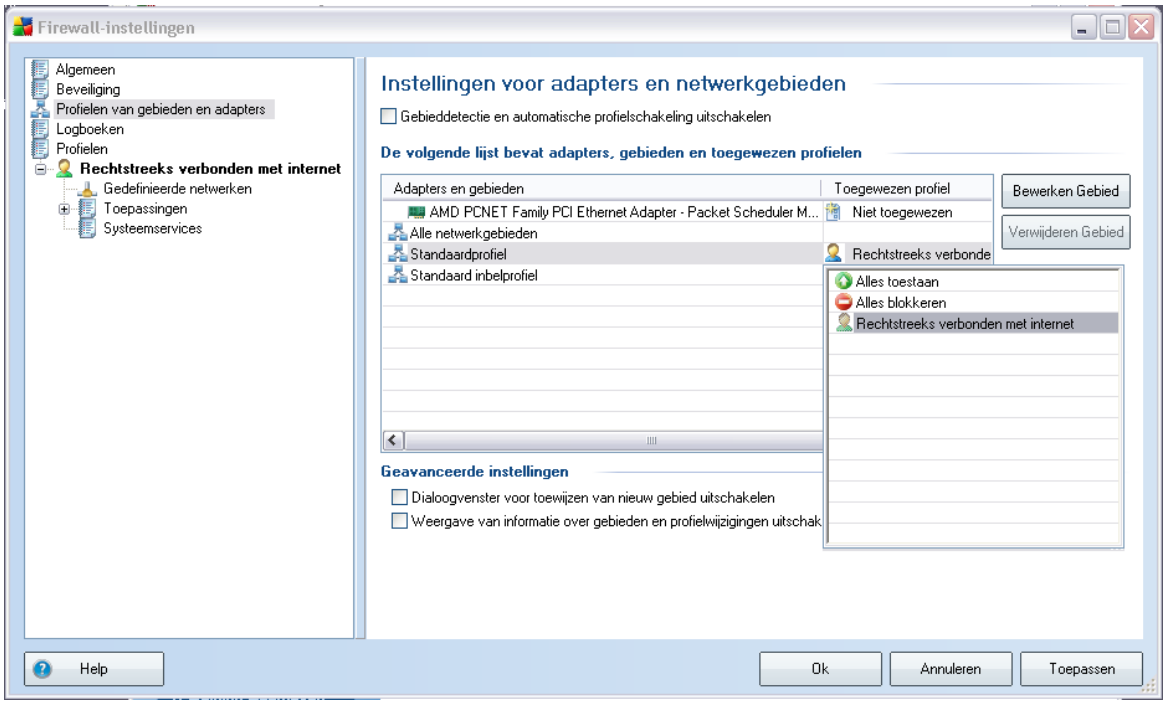
Voor beide opties kunt u het specifieke recht toewijzen aan een van de volgende gebruikersgroepen:

- ***Beheerder*** – de beheerder heeft volledige controle over de pc en kan iedere gebruiker in groepen indelen met specifiek gedefinieerde rechten
- ***Beheerder en hoofdgebruiker*** – de beheerder kan iedere gebruiker in

een specifieke groep (*Hoofdgebruiker*) indelen en rechten voor de groepsleden definiëren

- ***Alle gebruikers*** – andere gebruikers die niet aan een specifieke groep zijn toegewezen

11.3. Profielen van gebieden en adapters



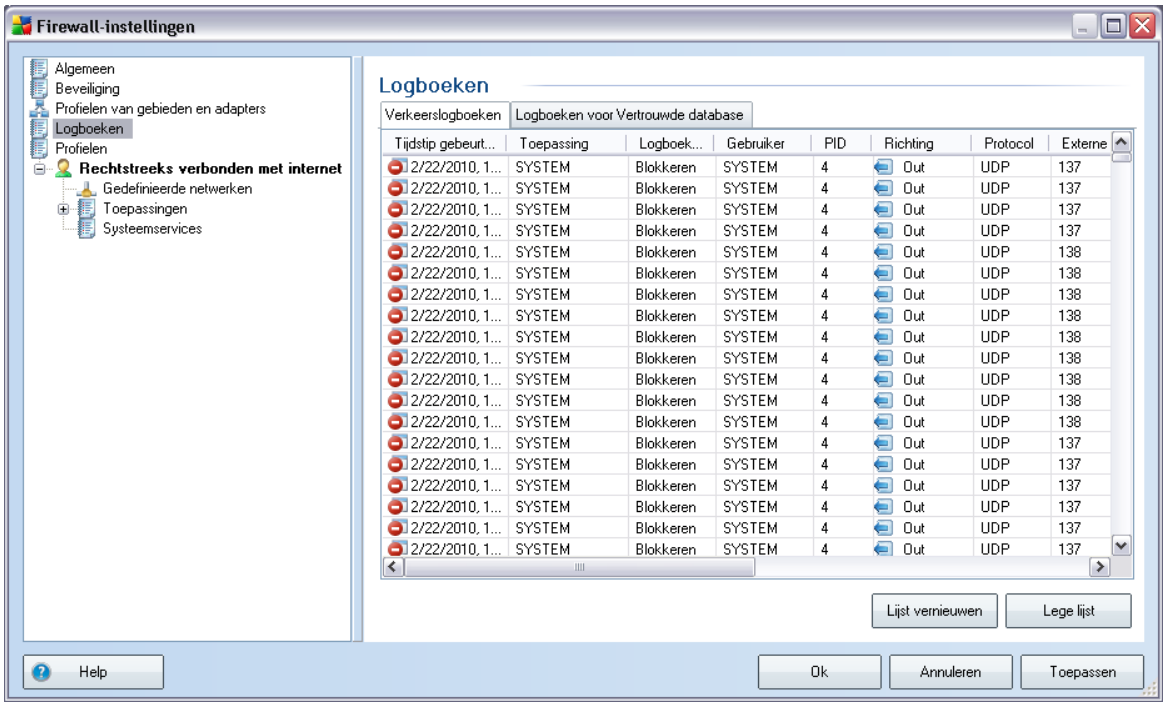
In het dialoogvenster ***Instellingen voor adapters en netwerkgebieden*** kunt u instellingen opgeven die betrekking hebben op het toewijzen van vooraf gedefinieerde profielen aan specifieke adapters en de bijbehorende netwerken:

- ***Gebieddetectie en automatische profielschakeling uitschakelen*** - één van de gedefinieerde profielen kan worden toegewezen aan elk type netwerkinterface, respectievelijk aan elk gebied. Als u geen specifieke profielen wilt definiëren, wordt een algemeen profiel dat is samengesteld op basis van uw selectie voor computergebruik en opzet van uw computernetwerk tijdens de ***installatieprocedure*** gebruikt. Als u echter onderscheid wilt maken tussen profielen en ze wilt toewijzen aan specifieke adapters en gebieden en dan achteraf, om de één of andere reden, die ordening tijdelijk wilt wijzigen, schakelt u het selectievakje ***Gebieddetectie en profielschakeling uitschakelen*** in.

- ***Lijst met gebieden en toegewezen profielen*** - deze lijst biedt een overzicht van gedetecteerde adapters en gebieden. U kunt elk van hen een specifiek profiel toewijzen uit het menu met gedefinieerde profielen. Klik op een item in de lijst met adapters om het menu te openen en selecteer dan een profiel.

- ***Geavanceerde instellingen*** - als u de opties inschakelt, zullen dialoogvensters voor nieuwe gebieden en meldingen niet meer worden weergegeven.

11.4. Logboeken



In het dialoogvenster ***Logboeken*** kunt u op twee tabbladen een lijst met alle geregistreerde ***Firewall***-acties en -gebeurtenissen bekijken met een gedetailleerde beschrijving van de relevante parameters (*tijdstip gebeurtenis, toepassingsnaam, desbetreffende logboekactie, gebruikersnaam, PID, verkeersrichting, protocoltype, nummers van de externe en lokale poorten, enzovoort*):

- ***Verkeersmeldingen*** - informatie over activiteiten van alle toepassingen die hebben geprobeerd verbinding te maken met het netwerk.

- ***Meldingen Vertrouwde database*** - de *Vertrouwde database* is de interne database van AVG waarin informatie wordt verzameld over gecertificeerde en

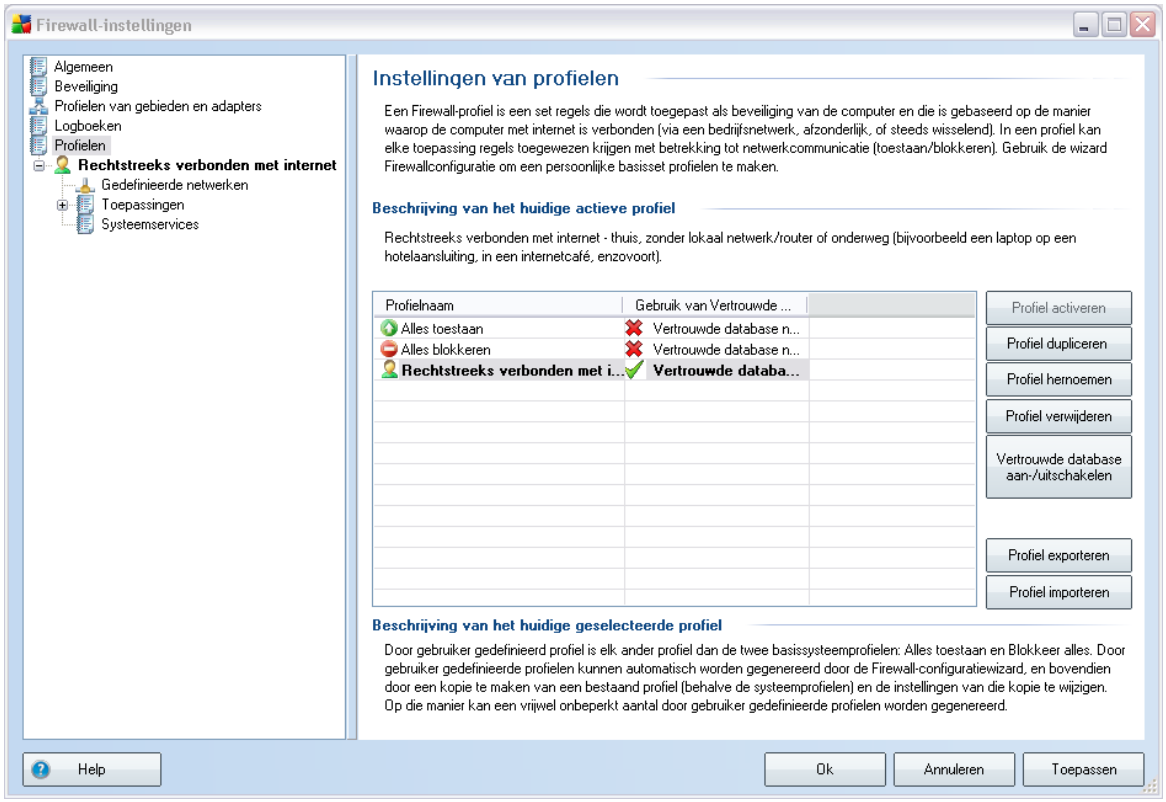
vertrouwde toepassingen die altijd mag worden toegestaan online te communiceren. De eerste keer dat een nieuwe toepassing probeert een verbinding tot stand te brengen met het netwerk (*terwijl er bijvoorbeeld nog geen Firewall-regel voor de toepassing is gedefinieerd*), moet worden uitgezocht of de desbetreffende 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, wanneer 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

- ***Help*** - De Help bij het dialoogvenster wordt weergegeven.
- ***Lijst vernieuwen***- alle vastgelegde parameters kunnen worden gesorteerd op een geselecteerde eigenschap: chronologisch (*datums*) of alfabetisch (*andere kolommen*) door op de kolomkop te klikken. Klik op de knop ***Lijst vernieuwen*** om de weergegeven informatie up-to-date te maken.
- ***Lijst leegmaken*** - alle items in het diagram wissen.

11.5. Profielen

In het dialoogvenster ***Instellingen van profielen*** staat een lijst met alle beschikbare profielen.



Alle andere dan de systeemprofielen kunnen in dit dialoogvenster worden gewijzigd met behulp van de volgende knoppen:

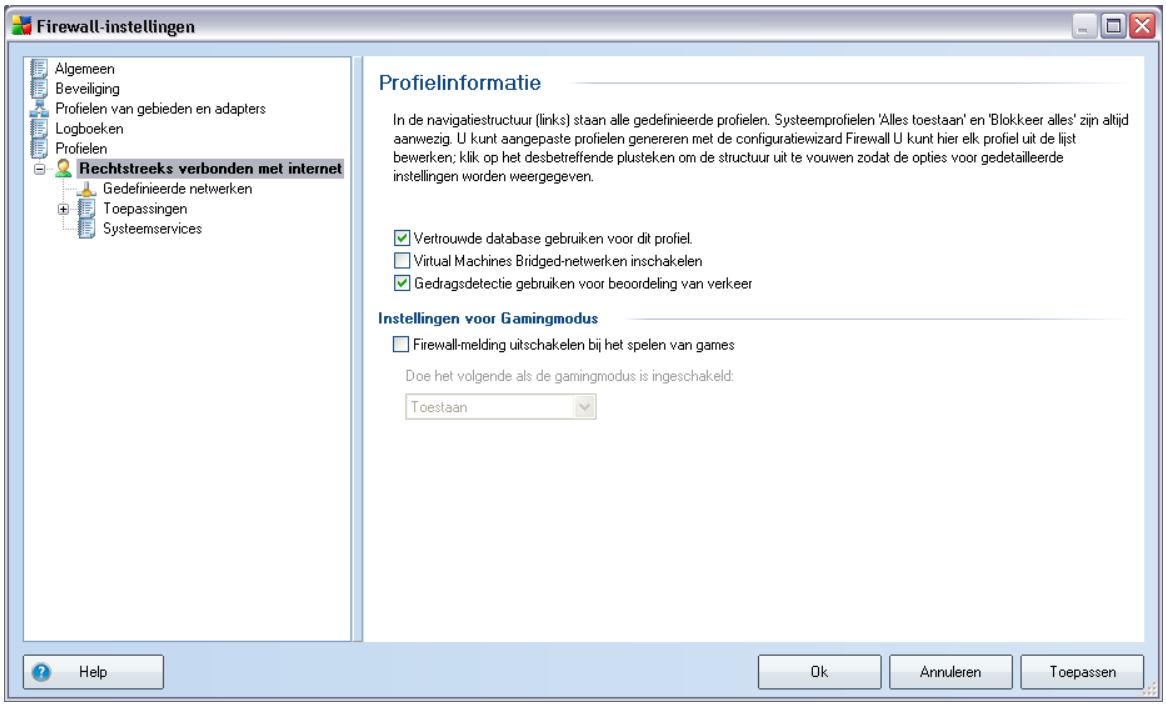
- ***Profiel activeren*** - met deze knop stelt u het geselecteerde profiel in als actief profiel, dat wil zeggen dat de geselecteerde profielconfiguratie zal worden gebruikt door de ***Firewall*** bij het controleren van het netwerkverkeer
- ***Profiel dupliceren*** - er wordt een identieke kopie gemaakt van het geselecteerde profiel; vervolgens kunt u de kopie bewerken en een andere naam geven en zo een nieuw profiel maken gebaseerd op het gedupliceerde origineel.
- ***Profiel hernoemen*** - het geselecteerde profiel een nieuwe naam geven

- ***Profiel verwijderen*** - het geselecteerde profiel uit de lijst verwijderen
- ***Vertrouwde database in-/uitschakelen*** - u kunt opgeven of u voor het geselecteerde profiel de informatie uit de *Vertrouwde database* wilt gebruiken (*Vertrouwde database is de interne database van AVG waarin informatie wordt verzameld over gecertificeerde en vertrouwde toepassingen die altijd mag worden toegestaan online te communiceren.*)
- ***Profiel exporteren*** - de configuratie van het geselecteerde profiel wordt opgeslagen in een bestand en kan in die vorm verder worden gebruikt
- ***Profiel importeren*** - de instellingen van het geselecteerde profiel worden geconfigureerd overeenkomstig de gegevens die worden opgehaald uit het back-upconfiguratiebestand
- ***Help*** - De Help bij het dialoogvenster wordt weergegeven

Onder in het dialoogvenster staat een beschrijving van het in de lijst erboven geselecteerde profiel.

De navigatiestructuur links in het dialoogvenster ***Profiel*** wordt aangepast overeenkomstig het aantal gedefinieerde profielen in de lijst rechts in het dialoogvenster. Elk gedefinieerd profiel wordt als een afzonderlijke vertakking van het item ***Profiel*** in de navigatiestructuur weergegeven. Profielen kunnen worden bewerkt in de volgende dialoogvensters (*de dialoogvensters zijn voor alle profielen gelijk*):

11.5.1. Profielinformatie



Het dialoogvenster ***Profielinformatie*** is het eerste van een reeks voor het bewerken van profielgegevens in dialoogvensters die elk zijn gericht op specifieke parameters van het profiel.

- ***Vertrouwde database gebruiken voor dit profiel*** - (*standaard ingeschakeld*) schakel dit selectievakje in om de *Vertrouwde database* in te schakelen (*dat is de database waarin informatie wordt opgeslagen over vertrouwde en gecertificeerde toepassingen die online communiceren. Als er nog geen regel voor de desbetreffende toepassing is gedefinieerd, moet worden uitgezocht of de toepassing toegang mag krijgen tot het netwerk. AVG heeft eerst de Vertrouwde database doorzocht, en als de toepassing daarin wordt vermeld, zal hij als veilig worden beschouwd en wordt toestemming verleend om via het netwerk te communiceren. Zo niet, dan wordt u gevraagd een beslissing te nemen of de toepassing mag worden toegestaan te communiceren via het netwerk*) binnen het desbetreffende profiel

- ***Virtual Machines Bridged-netwerken inschakelen***- (*standaard uitgeschakeld*) schakel dit selectievakje in om directe aansluiting van virtuele machines in WMware op het netwerk toe te staan

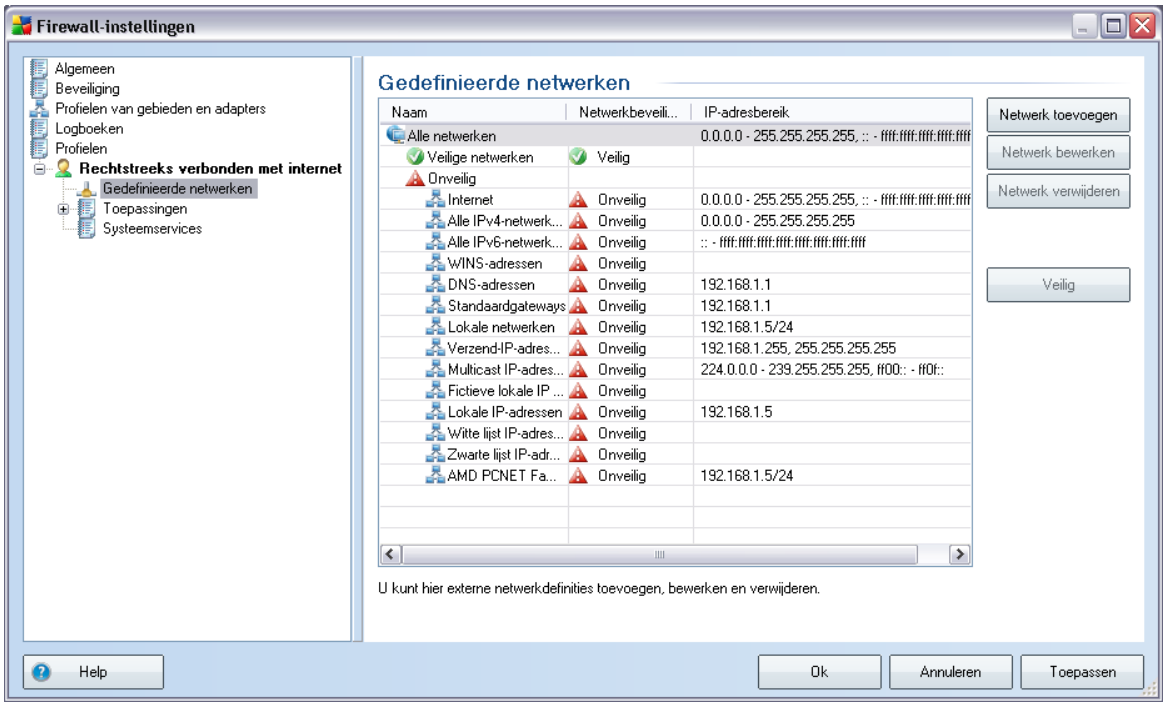
- ***Gedragsdetectie gebruiken voor beoordeling van verkeer*** - (*standaard ingeschakeld*) schakel dit selectievakje in om ***Firewall*** toe te staan ***Identity Protection***-functionaliteit te gebruiken bij het beoordelen van een toepassing - ***Identity Protection***kan oordelen of een toepassing verdacht gedrag vertoont, of kan worden vertrouwd en kan worden toegestaan online te communiceren.

Instellingen voor Gamingmodus

In het gedeelte ***Instellingen voor Gamingmodus*** kunt u met behulp van het selectievakje aangeven of meldingen van de ***Firewall***moeten worden weergegeven, als toepassingen schermvullend worden uitgevoerd op de computer (*gewoonlijk gaat het dan om games, maar de instelling geldt ook voor andere schermvullende toepassingen, bijvoorbeeld PowerPoint-presentaties*). Aangezien de informatieberichten enigszins ontregelend kunnen zijn.

Als u het selectievakje ***Firewall-melding uitschakelen bij het spelen van games*** inschakelt, kunt u in het vervolgkeuzemenu aangeven wat er moet gebeuren als een nieuwe toepassing, waarvoor nog geen regels zijn ingesteld, probeert te communiceren via het netwerk (*toepassingen waarvoor normaal gesproken onder dergelijke omstandigheden een dialoogvenster wordt geopend*); u kunt die toepassingen toestaan of blokkeren.

11.5.2. Gedefinieerde netwerken

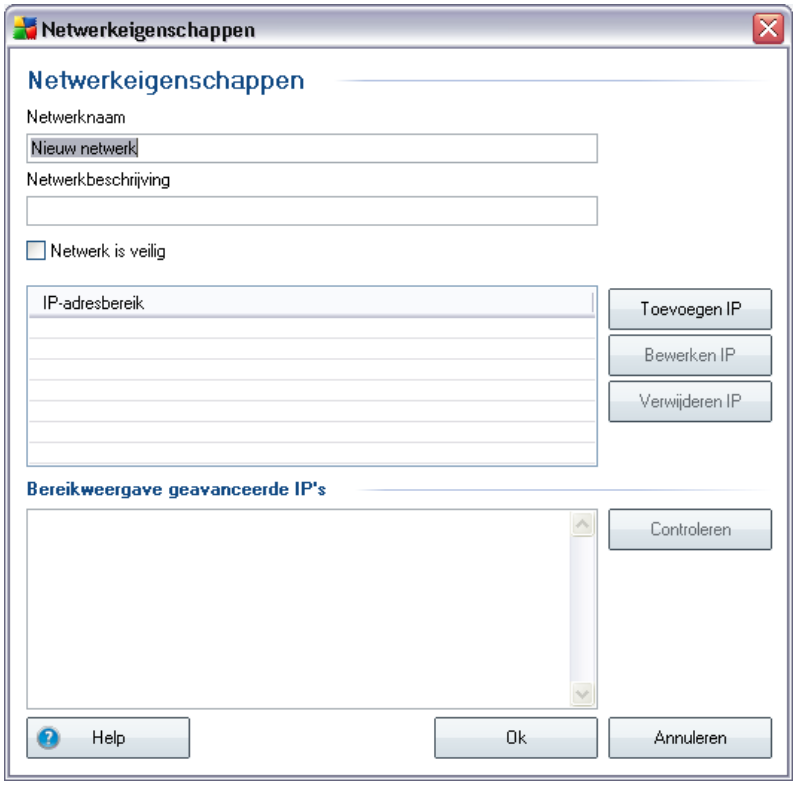


In het dialoogvenster ***Gedefinieerde netwerken*** staat een lijst met alle netwerken waarop uw computer is aangesloten. Voor elk gedetecteerde netwerk wordt de volgende informatie weergegeven:

- ***Netwerken*** - de lijst met namen van netwerken waarop de computer is aangesloten
- ***Netwerkbeveiliging*** - standaard worden alle netwerken als onveilig beschouwd, en alleen als u zeker weet dat een netwerk veilig is, kunt u het als zodanig instellen (*klik in de lijst op het desbetreffende netwerk en selecteer Veilig in het snelmenu*) - alle veilige netwerken worden dan toegevoegd aan de groep waarmee de toepassing kan communiceren met voor de toepassingsregel de instelling Toestaan als veilig
- ***IP-adresbereik*** - elk netwerk wordt automatisch gedetecteerd en weergegeven in de vorm van een IP-adresbereik

Knoppen

- ***Netwerk toevoegen*** - het dialoogvenster ***Netwerkeigenschappen*** wordt geopend waarin u parameters kunt instellen voor het nieuw gedefinieerde netwerk:



In dit dialoogvenster kunt u de ***Netwerknaam*** en een ***Netwerkbeschrijving*** opgeven, en mogelijk het netwerk instellen als veilig. U kunt het nieuwe netwerk handmatig definiëren in een standalone dialoogvenster ***IP toevoegen***(dan wel ***IP bewerken*** / ***IP verwijderen***), in dit dialoogvenster kunt u het netwerk specificeren aan de hand van het IP-adresbereik of het masker.

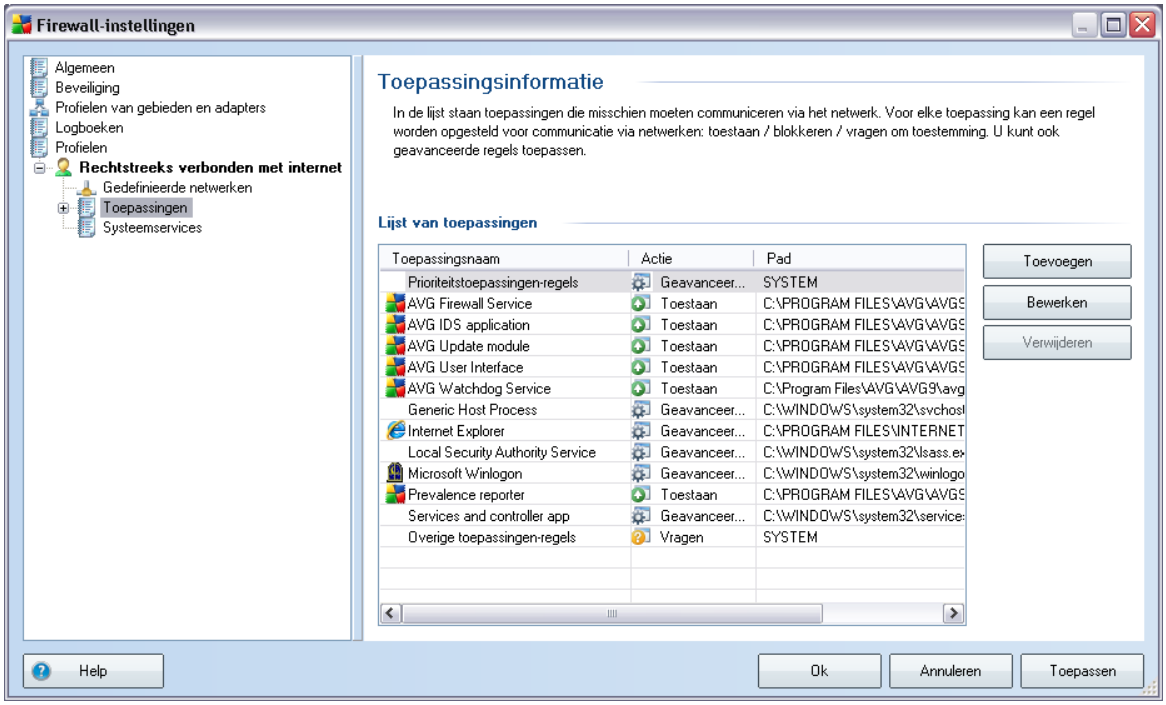
Als een groot aantal netwerken moet worden gedefinieerd als onderdeel van het nieuw gecreëerde netwerk, kunt u gebruikmaken van de optie ***Geavanceerde weergave IP-bereik***: voer de lijst met netwerken in in het desbetreffende tekstvak (*elke standaardopmaak wordt ondersteund*) en klik op de knop***Controleren*** om te controleren of de opmaak wordt herkend. Klik vervolgens op ***OK*** om de invoer te bevestigen en de gegevens op te slaan.

- ***Netwerk bewerken*** - het dialoogvenster ***Netwerkeigenschappen*** wordt

geopend (*zie hiervoor*) waarin u de parameters van eerder gedefinieerd netwerk kunt bewerken (*het dialoogvenster is gelijk aan het dialoogvenster voor het toevoegen van een nieuw netwerk, zie de beschrijving in de vorige paragraaf*)

- ***Netwerk verwijderen*** - het geselecteerde netwerk wordt uit de lijst verwijderd.
- ***Markeren als Veilig*** - standaard worden alle netwerken als onveilig beschouwd, en alleen als u zeker weet dat een netwerk veilig is, kunt u het als zodanig instellen met deze knop (*als het netwerk als veilig is gemarkeerd, verandert deze knop in "Markeren als Onveilig"*).
- ***Help*** - de Help bij het dialoogvenster wordt weergegeven

11.5.3. Toepassingen



In het dialoogvenster ***Toepassingsinformatie*** staan alle geïnstalleerde toepassingen die wellicht moeten communiceren via het netwerk, samen met pictogrammen voor de toegewezen acties:

- Communicatie toestaan voor alle netwerken

-  Alleen communicatie toestaan voor netwerken die zijn aangemerkt als veilig
-  Communicatie blokkeren
-  Bevestigingsdialoog weergeven (*de gebruiker wordt op het moment dat het aan de orde is gevraagd of hij de communicatie wil toestaan of blokkeren*)
-  Geavanceerde instellingen gedefinieerd

De toepassingen in de lijst zijn op uw computer gedetecteerd (*en hebben acties toegewezen gekregen*) tijdens het zoeken door de ***Wizard Firewallconfiguratie***, of op een later tijdstip als het gaat om een onbekende, of later toegevoegde toepassing.

Opmerking: bij de uitvoering van de Wizard Firewallconfiguratie zijn alleen toepassingen gedetecteerd die op dat moment al waren geïnstalleerd; dat betekent dat u bij installatie van een toepassing op een later tijdstip, alsnog Firewall-regels voor die toepassing zult moeten opstellen. Standaard zal de Firewall als de nieuwe toepassing voor het eerst probeert een verbinding tot stand te brengen via het netwerk, automatisch een regel maken voor de toepassing in overeenstemming met de Vertrouwde database, of u vragen of u toestemming wilt verlenen voor de communicatie of die wilt 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 de regels voor de nieuwe toepassing ook meteen definiëren - klik daartoe in dit dialoogvenster op ***Toevoegen*** en voer de parameters voor de toepassing in.

Behalve de toepassingen staan er twee speciale items in de lijst:

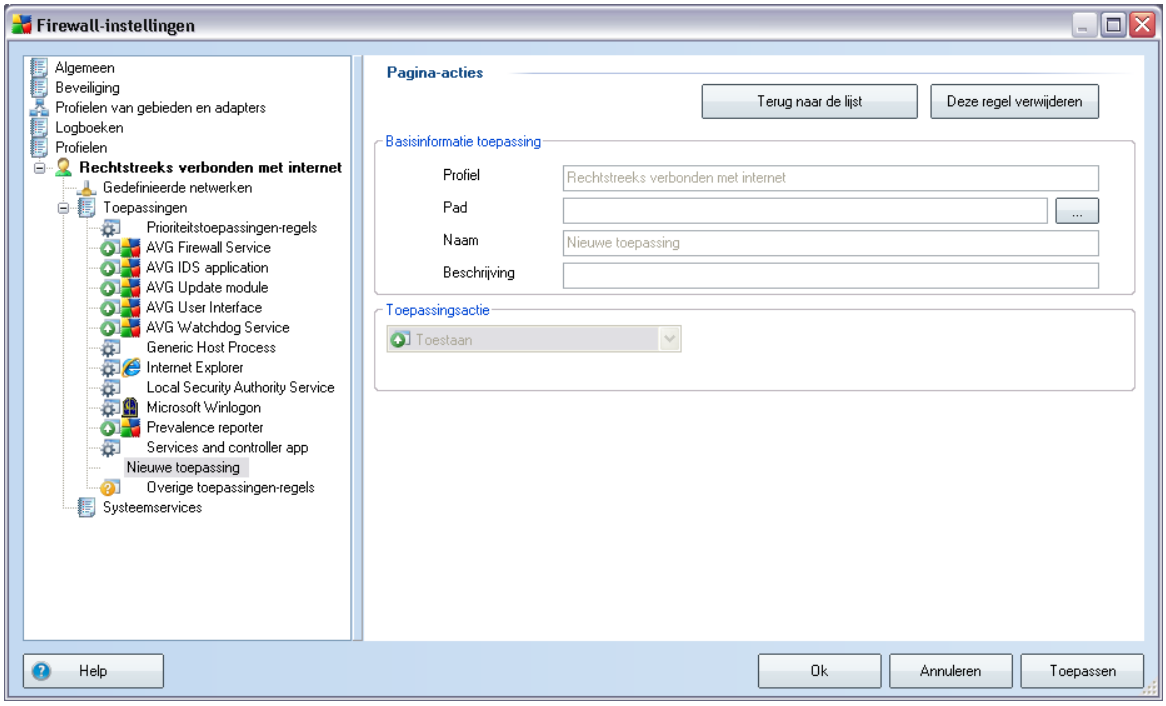
- ***Prioriteit toepassingsregels*** (*bovenaan de lijst*) zijn voorkeursregels die altijd worden toegepast met voorrang op de regels van afzonderlijke toepassingen.
- ***Overige toepassingsregels***(*(onderaan de lijst*) zijn regels die "in laatste instantie" worden toegepast als er geen specifieke toepassingsregels zijn, dus bij onbekende en niet-gedefinieerde toepassingen.

Deze items hebben andere opties voor instellingen dan de doorsnee toepassingen, en zijn alleen bedoeld voor ervaren gebruikers. Wij adviseren u met klem om deze instellingen niet te wijzigen

Knoppen

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

- ***Toevoegen*** - opent een leeg dialoogvenster ***Pagina-acties*** waarin u nieuwe toepassingsregels kunt opgeven
- ***Bewerken*** - opent het dialoogvenster ***Pagina-acties*** met daarin gegevens voor bestaande toepassingsregels die u kunt bewerken
- ***Verwijderen*** - de geselecteerde toepassing verwijderen uit de lijst
- ***Help*** - de Help bij het dialoogvenster wordt weergegeven



In dit dialoogvenster kunt u gedetailleerde instellingen opgeven voor de desbetreffende toepassing.

Pagina-acties

- Δεκνοπ ***Terug naar de lijst*** geeft een overzicht van alle gedefinieerde toepassingsregels.

- Δεκνοπ ***Deze regel verwijderen*** verwijdert de op dat moment weergegeven toepassingsregel. Let op:die handeling kan niet meer ongedaan worden gemaakt!

Basisinformatie toepassing

Geef in dit gedeelte de ***naam*** op van de toepassing en eventueel een ***beschrijving*** (*beknopt commentaar voor uzelf*). Typ in het veld ***Pad*** het volledige pad naar de toepassing (*het uitvoerbare bestand*) op de schijf; u kunt de toepassing ook opzoeken in de bestandsstructuur als u op de knop "***...***" klikt.

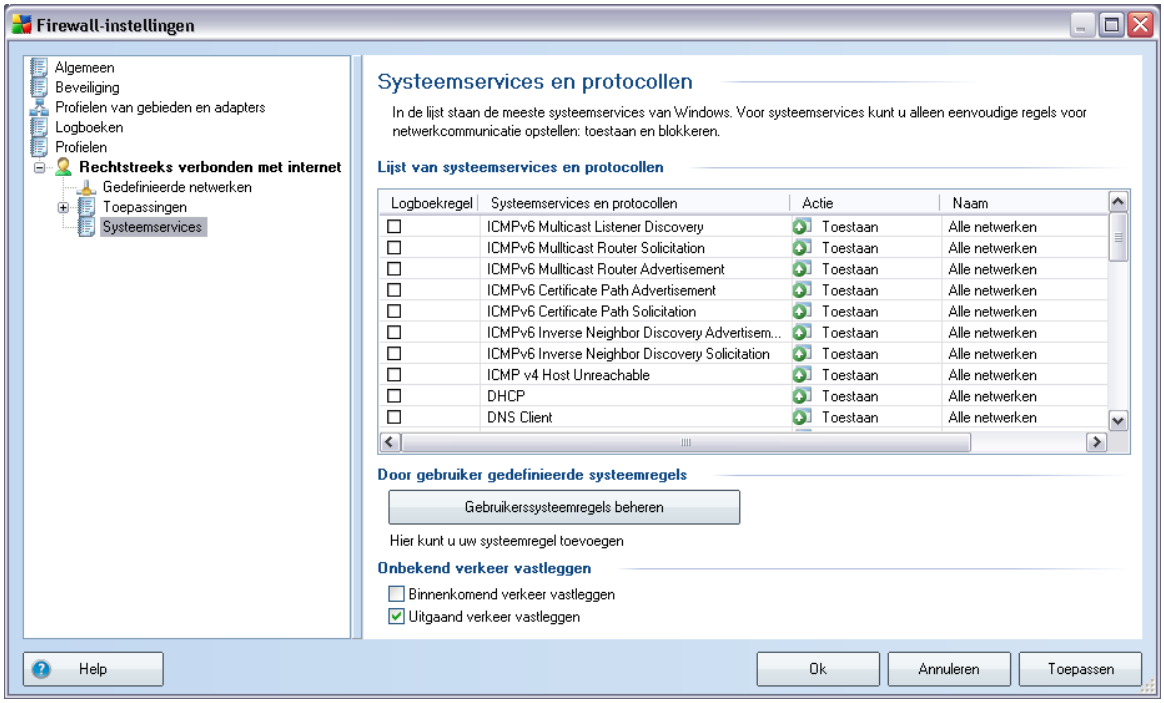
Toepassingsactie

In de vervolgkeuzelijst kunt u de Firewall-regel voor de toepassing selecteren, dat wil zeggen de actie die Firewall moet ondernemen wanneer de toepassing via het netwerk probeert te communiceren:

- ***Alles toestaan*** het wordt de toepassing, zonder enige beperking, toegestaan te communiceren via alle bekende netwerken en adapters.
- ***Toestaan als veilig*** de toepassing mag alleen communiceren via netwerken die als veilig (betrouwbaar) zijn aangemerkt.
- ***Blokkeren*** de communicatie wordt automatisch verboden; de toepassing mag niet communiceren met enig netwerk.
- ***Vragen*** er wordt een dialoogvenster geopend, waarin u bepaalt of u op dat moment de communicatie wilt toestaan of blokkeren.
- Iv ***Geavanceerde instellingen*** in het onderste gedeelte van het dialoogvenster in de sectie ***Toepassingsonderdeelregels*** vindt u nog meer gedetailleerde instellingsopties. De gedetailleerde regels worden toegepast naar rangorde van de lijst, dus u kunt de regels ***Omhoog verplaatsen*** en ***Omlaag verplaatsen*** in de lijst, al naar gelang de prioriteit. Als u op een regel in de lijst klikt, wordt een overzicht van de regeldetails weergegeven in het onderste deel van het dialoogvenster. Alle blauw onderstreepte waarden kunt u wijzigen als u in het desbetreffende dialoogvenster Instellingen klikt. Als u een geselecteerde regel wilt verwijderen, klikt u op ***Verwijderen***. Als u een nieuwe regel wilt definiëren, klikt u op de knop ***Toevoegen*** om het dialoogvenster ***Regeldetail wijzigen*** te openen waarin u alle noodzakelijke details kunt opgeven.

11.5.4. Systeemservices

We raden u met nadruk 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:

- ***Regelactie registreren*** - als u dit selectievakje inschakelt, wordt elke toepassing van een regel vastgelegd in de Logboeken.
- ***Systeemservices en protocollen*** - deze kolom bevat de naam van de desbetreffende systeemservice.
- ***Actie*** - in deze kolom wordt een pictogram voor de toegewezen actie weergegeven:
    - o Communicatie toestaan voor alle netwerken
    - o Alleen communicatie toestaan voor netwerken die zijn aangemerkt als veilig

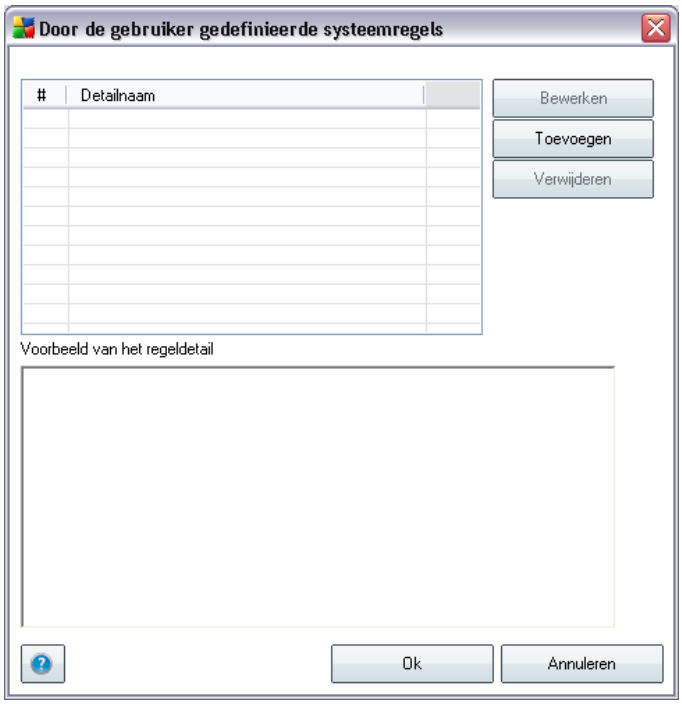
- Communicatie blokkeren

- ***Netwerken*** - in deze kolom staat op welk specifiek netwerk de systeemregel van toepassing is.

U kunt de lijst (*inclusief de toegewezen acties*) bewerken met behulp van de volgende knoppen:

- 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***.

- 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***. Het bovenste deel van het dialoogvenster ***Door de gebruiker gedefinieerde systeemregels*** bevat een overzicht van alle details van de systeemregel die op dat moment wordt bewerkt; in het onderste deel wordt het geselecteerde detail weergegeven. Door gebruiker gedefinieerde regeldetails kunnen worden bewerkt, toegevoegd of verwijderd met de desbetreffende knoppen; programma-eigen regeldetails kunnen alleen worden bewerkt:



Waarschuwing: *Het gaat hier om geavanceerde instellingen, vooral bedoeld voor netwerkbeheerders die de volledige 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.*

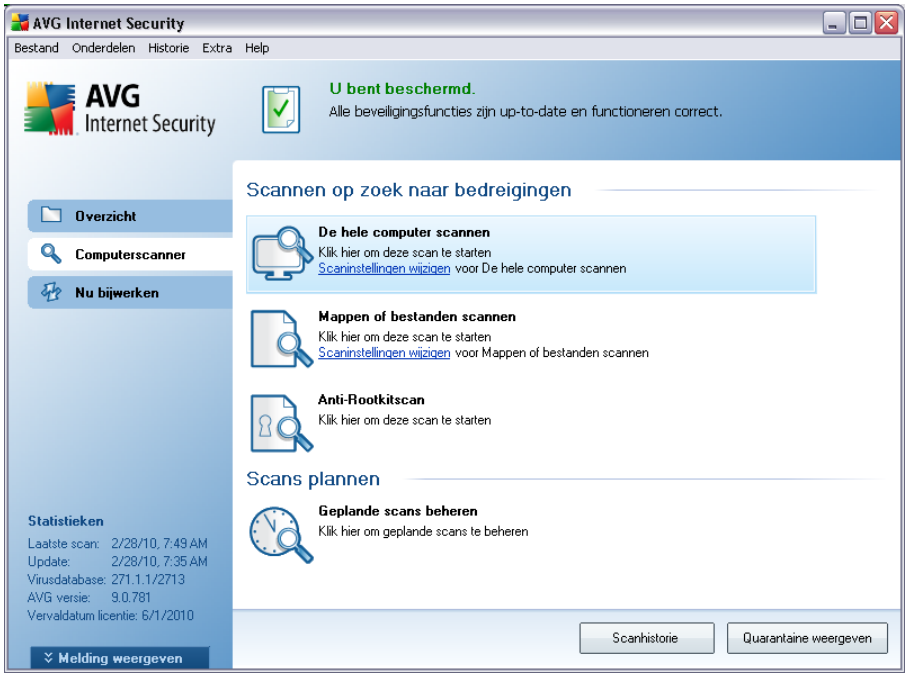
Onbekend verkeer vastleggen

- ***Onbekend binnenkomend verkeer vastleggen*** - schakel het selectievakje in om in de logboeken elke onbekende poging van buitenaf om contact te leggen met uw computer, te registreren.
- ***Onbekend uitgaand verkeer vastleggen*** - schakel het selectievakje in om in delogboeken elke onbekende poging van uw computer om contact te leggen met de buitenwereld, te registreren.

12. AVG scannen

Scannen is een essentieel onderdeel van de functionaliteit van **AVG 9 Internet Security**. U kunt tests op verzoek uitvoeren of u kunt ze plannen, zodat ze periodiek worden uitgevoerd op tijdstippen waarop het u schikt

12.1. Scaninterface



U kunt de AVG interface voor het scannen oproepen via de snelkoppeling ***Computerscanner***. Klik op die koppeling om het dialoogvenster ***Scannen op zoek naar bedreigingen*** te openen. In dat dialoogvenster treft u het volgende aan:

- overzicht van vooraf gedefinieerde scans - drie typen door de leverancier van de software gedefinieerde scans, die u meteen kunt gebruiken of plannen:
  - ***De hele computer scannen***
  - ***Bepaalde mappen of bestanden scannen***
  - ***Anti-Rootkitscan***
- scans plannen - naar wens definiëren van nieuwe tests en plannen van tests.

Knoppen

De testinterface heeft de volgende knoppen:

- ***Scanhistorie*** - weergave van het dialoogvenster Overzicht scanresultaten met de volledige scanhistorie
- ***Quarantaine weergeven*** - er wordt een nieuw venster geopend met de Quarantaine - een opslagruimte waar gedetecteerde infecties worden opgeslagen

12.2. Vooraf ingestelde scans

Een van de belangrijkste voorzieningen van **AVG 9 Internet Security** is de mogelijkheid om op verzoek scans uit te voeren. De tests 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 tests regelmatig uitvoeren. Dat geldt ook als u vermoedt dat er geen virussen op uw computer zullen worden gevonden.

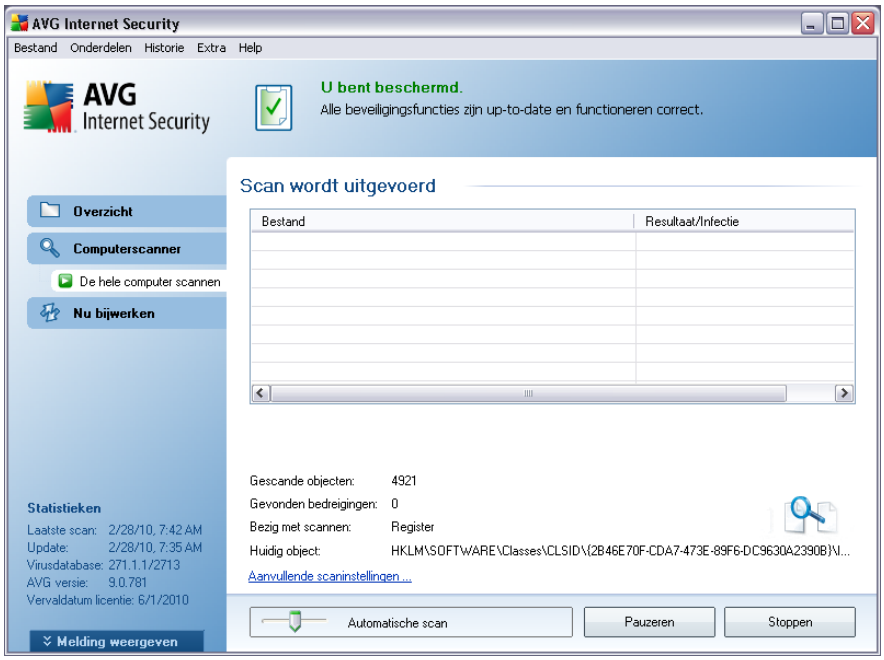
AVG 9 Internet Security bevat twee scanmethodes die door de softwareleverancier van te voren zijn gedefinieerd:

12.2.1. De hele computer scannen

De hele computer scannen - de hele computer wordt gescand op mogelijke infecties en/of potentieel ongewenste programma'sP Alle vaste schijven van de computer worden gescand, alle virussen worden gedetecteerd en hersteld of verplaatst naar de ***Quarantaine***. Een scan van de hele computer dient op een werkstation minstens eenmaal per week te worden uitgevoerd.

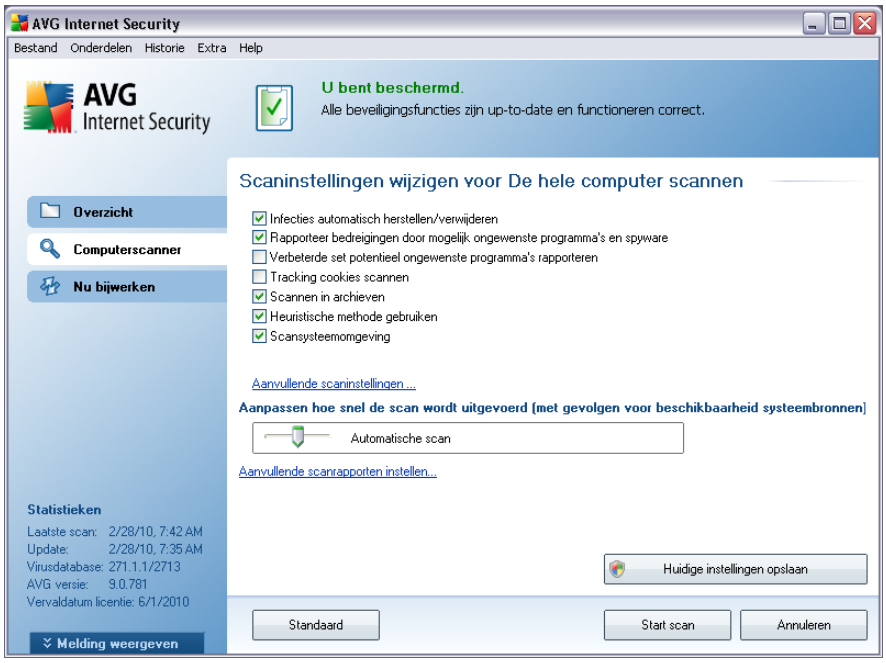
Scan starten

U kunt ***De hele computer scannen*** direct vanuit de scaninterface starten door op het pictogram van de scan te klikken. U hoeft verder geen instellingen op te geven voor dit type scan, het scannen wordt onmiddellijk gestart in het dialoogvenster ***Scan wordt uitgevoerd*** (*zie schermafbeelding*). U kunt het scanproces tijdelijk onderbreken (***Onderbreken***) en afbreken (***Stoppen***), als dat nodig is.



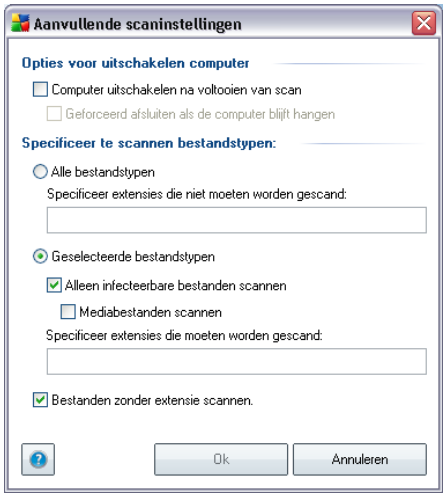
Scanconfiguratie bewerken

U kunt de vooraf gedefinieerde standaardinstellingen van ***De hele computer scannen*** wijzigen. Klik op de koppeling ***Scaninstellingen wijzigen*** om het dialoogvenster ***Scaninstellingen wijzigen voor De hele computer scannen*** te openen. ***Het is raadzaam de standaardinstellingen aan te houden, tenzij u een goede reden hebt om ze te wijzigen!***



- ***Scanparameters*** - in de lijst met scanparameters kunt u scanparameters naar wens in- en uitschakelen. Standaard zijn de meeste parameters ingeschakeld, zodat ze bij het scannen automatisch worden toegepast.

- ***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 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***).

- ***Specificeer te scannen bestandstypen*** - geef op wat u precies wilt scannen:

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

  - ***Geselecteerde bestandstypen*** - u kunt opgeven dat u alleen bestanden wilt scannen die mogelijk 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, reduceert 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 aan de hand 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 uitermate verdacht en dienen altijd te worden gescand.

- ***Prioriteit scanproces*** - met de schuifbalk kunt u de prioriteit voor het scanproces wijzigen. Standaard is de prioriteit ingesteld op gemiddeld (*Automatische scan*), waarbij de snelheid van het scanproces en het gebruik van systeembronnen (o.a. het werkgeheugen van uw computer) optimaal op elkaar zijn afgesteld. 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 geopend, ***Scanrapporten***, waarin u kunt aangeven wat voor soort resultaten moeten worden gerapporteerd:

Waarschuwing: *deze scaninstellingen zijn gelijk aan die van een nieuwe gedefinieerde scan - zoals beschreven in het hoofdstuk* ***AVG scannen / Scans plannen / Hoe er gescand moet worden****. 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.*

12.2.2. Bepaalde mappen of bestanden scannen

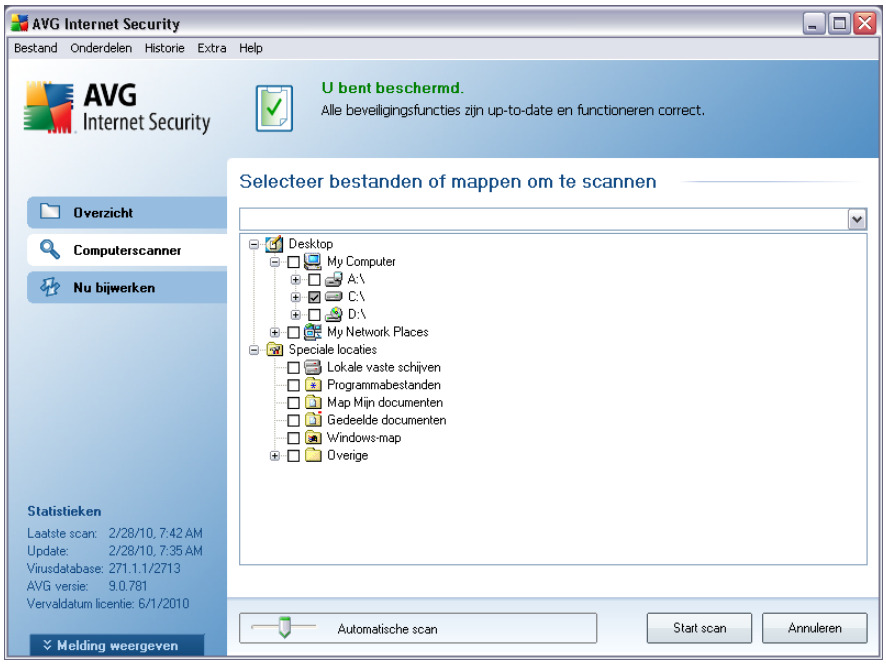
Bepaalde mappen of bestanden scannen - alleen die gebieden worden gescand die u hebt geselecteerd voor het scannen *(geselecteerde mappen, vaste schijven, diskettes, cd's, enz.*). De voortgang bij het scannen in het geval dat een virus wordt gedetecteerd, en de manier waarop het virus wordt behandeld, 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

U kunt ***Bepaalde mappen of bestanden scannen*** direct vanuit de scaninterface starten door op het pictogram van de scan te klikken. Er wordt een nieuw dialoogvenster, ***Selecteer bestanden of mappen om te scannen***, geopend. Selecteer in de bestandsstructuur van de computer die mappen die u wilt scannen. Het pad naar elke geselecteerde map wordt automatisch gegenereerd en weergegeven in het tekstvak in het bovenste deel van het dialoogvenster.

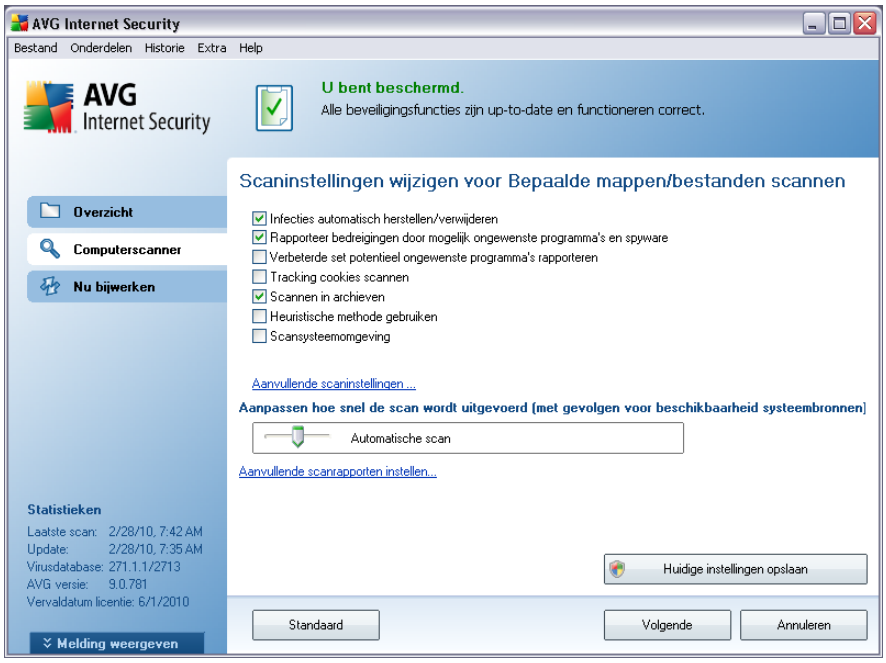
U kunt ook een map scannen, maar tegelijkertijd alle submappen van die map uitsluiten van het scannen; daartoe typt u een minteken "**-**" voor het automatisch gegenereerde pad (*zie de schermafbeelding*). Als u de hele map wilt uitsluiten van het scannen, gebruikt u de "!"- parameter.

Om uiteindelijk het scanproces te starten klikt u op de knop***Scannen starten***; het scanproces zelf is in principe gelijk aan het scanproces van Volledige computer scannen.



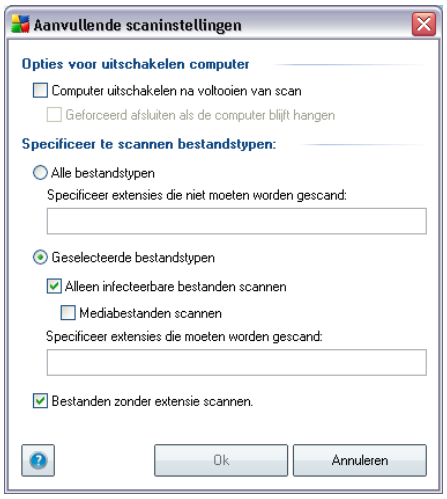
Scanconfiguratie bewerken

U kunt de vooraf gedefinieerde standaardinstellingen van ***Bepaalde mappen of bestanden scannen***wijzigen. Klik op de koppeling ***Scaninstellingen wijzigen*** om het dialoogvenster ***Scaninstellingen wijzigen voor Bepaalde mappen of bestanden scannen*** te openen. ***Het is raadzaam de standaardinstellingen aan te houden, tenzij u een goede reden hebt om ze te wijzigen!***



- ***Scanparameters*** - in de lijst met scanparameters kunt u naar wens parameters in- en uitschakelen (*zie voor een gedetailleerde beschrijving van deze instellingen in het hoofdstuk AVG Geavanceerde instellingen / Scans / Bepaalde mappen of bestanden scannen*).

- ***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 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***).

- ***Specificeer te scannen bestandstypen*** - geef op wat u precies wilt scannen:

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

  - ***Geselecteerde bestandstypen*** - u kunt opgeven dat u alleen bestanden wilt scannen die mogelijk 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, reduceert 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 aan de hand 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 uitermate verdacht en dienen altijd te worden gescand.

- ***Prioriteit scanproces*** - met de schuifbalk kunt u de prioriteit voor het scanproces wijzigen. Standaard is de prioriteit ingesteld op gemiddeld (*Automatische scan*), waarbij de snelheid van het scanproces en het gebruik van systeembronnen (o.a. het werkgeheugen van uw computer) optimaal op elkaar zijn afgesteld. 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 geopend, ***Scanrapporten***, waarin u kunt aangeven wat voor soort resultaten moeten worden gerapporteerd:

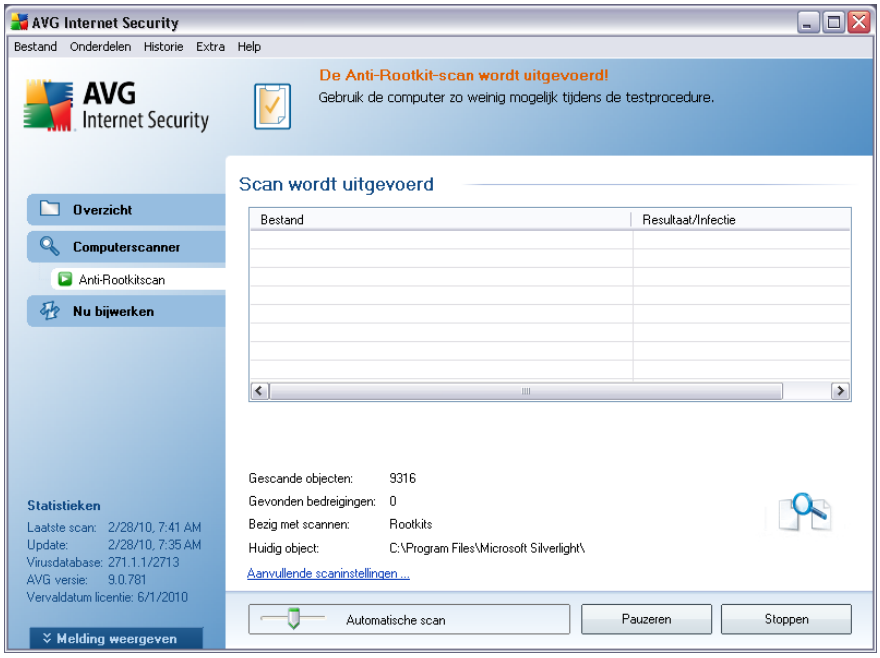
Waarschuwing: *deze scaninstellingen zijn gelijk aan die van een nieuwe gedefinieerde scan - zoals beschreven in het hoofdstuk* ***AVG scannen / Scans plannen / Hoe er gescand moet worden****. Mocht u besluiten de standaardconfiguratie van* ***Bepaalde mappen of bestanden scannen*** *te wijzigen, dan 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).*

12.2.3. Anti-rootkitscan

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.

Scan starten

Anti-Rootkitscan kan direct vanuit de scaninterface worden gestart door op het pictogram van de scan te klikken. U hoeft verder geen instellingen op te geven voor dit type scan, het scannen wordt onmiddellijk gestart in het dialoogvenster ***Scan wordt uitgevoerd*** (*zie schermafbeelding*). U kunt het scanproces tijdelijk onderbreken (***Onderbreken***) en afbreken (***Stoppen***), als dat nodig is.



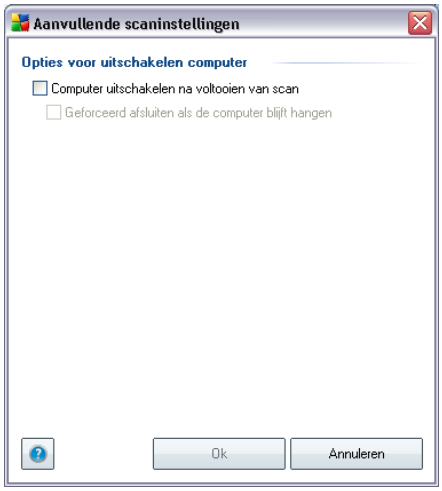
Scanconfiguratie bewerken

Anti-Rootkitscan wordt altijd gestart bij de standaardinstellingen, en bewerken van de scanparameters is alleen toegankelijk via het dialoogvenster ***AVG Geavanceerde instellingen / Anti-Rootkit***. In de scaninterface kunt u alleen het volgende configureren:

- ***Automatische scan*** - met de schuifbalk kunt u de prioriteit voor het scanproces wijzigen. Standaard is de prioriteit ingesteld op gemiddeld (*Automatische scan*), waarbij de snelheid van het scanproces en het gebruik van systeembronnen (o.a. het werkgeheugen van uw computer) optimaal op elkaar zijn afgesteld. 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*

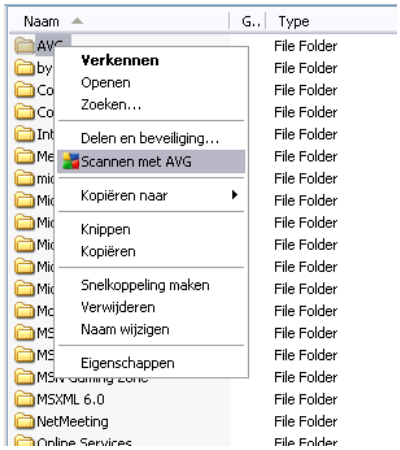
niet uitmaakt hoe lang het scanproces duurt), of sneller, waarbij een groter beroep wordt gedaan op systeembronnen (*bijvoorbeeld op een moment dat u de computer niet gebruikt*).

- ***Aanvullende scaninstellingen*** - er wordt een nieuw dialoogvenster ***Aanvullende scaninstellingen*** geopend, waarin u instellingen kunt opgeven voor het afsluiten van de computer met betrekking tot de ***Anti-Rootkitscan*** (***Computer uitschakelen na voltooien van scan****, of zelfs* ***Geforceerd afsluiten als de computer vergrendeld is***:



12.3. 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 9 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) die u wilt controleren
- Klik met de rechter muisknop op het object om het snelmenu te openen
- Kies de optie ***Met AVG scannen*** om het bestand te scannen met AVG

12.4. Scannen vanaf opdrachtregel

In **AVG 9 Internet Security** hebt u de mogelijkheid om een scan uit te voeren vanaf de opdrachtregel. Die optie kunt u 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.

Geef, als u AVG Scan vanaf de opdrachtregel wilt starten, de volgende opdracht 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 van elkaar gescheiden door een spatie en een slash

- Als een parameter bepaalde waarden vereist (bijv. de ***/scan***-parameter, 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 van elkaar gescheiden met puntkomma's, bijvoorbeeld: ***avgscanx /scan=C:\;D:***

Scanparameters

Als u een volledig overzicht wilt weergeven van beschikbare parameters, typt u de betreffende opdracht samen met 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 Windows Safe-modus, is er ook een mogelijkheid om de Opdrachtregel-scan te starten vanuit de grafische gebruikersinterface. De scan zelf wordt gestart vanaf de opdrachtregel. In het dialoogvenster ***Opdrachtregelcomposer*** kunt u slechts de meeste scanparameters specificeren in de comfortabele grafische interface.

Omdat dit dialoogvenster alleen toegankelijk is binnen de Windows Safe-modus raadpleegt u het helpbestand, dat direct wordt geopend vanuit het dialoogvenster, voor een gedetailleerde beschrijving van dit dialoogvenster.

12.4.1. CMD-scanparameters

Hieronder volgt een lijst met parameters die u bij het scannen vanaf de opdrachtregel kunt gebruiken:

- ***/SCAN*** Specifieke bestanden of mappen scannen /SCAN=path; path (e.g. /SCAN=C:\;D:\)

- ***/COMP*** De hele computer scannen

- ***/HEUR*** Heuristische analyse 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
- ***/MACROW*** Macro's in rapport opnemen
- ***/PWDW*** Bestanden met wachtwoordbeveiliging in rapport opnemen
- ***/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*** Scannen actieve processen
- ***/PUP*** "Potentieel ongewenste programma's" in rapport opnemen
- ***/REG*** Register scannen
- ***/COO*** Cookies scannen
- ***/?*** Help over dit onderwerp weergeven

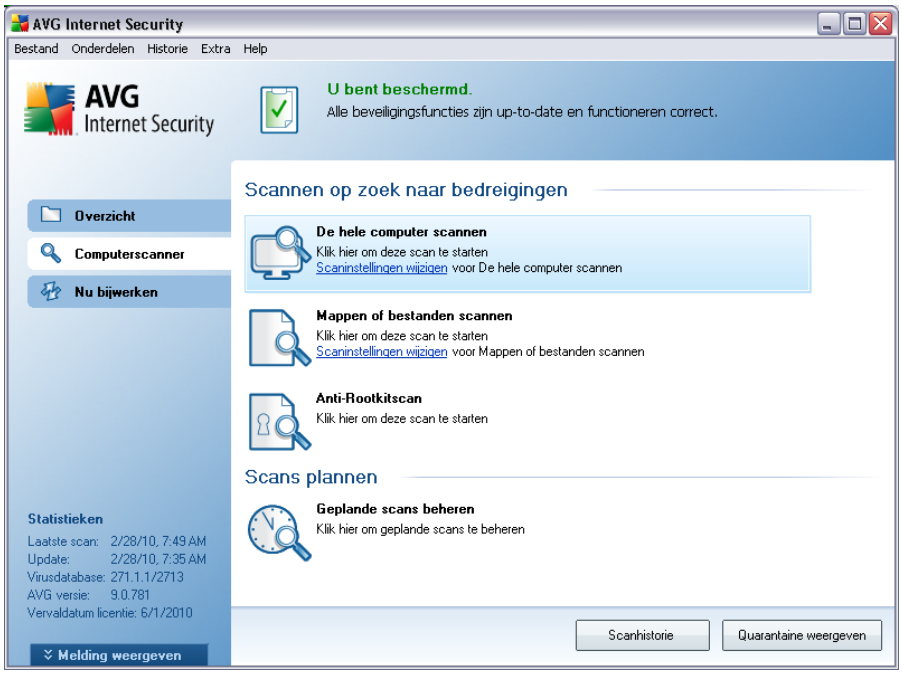
- ***/HELP*** Help over dit onderwerp weergeven
- ***/PRIORITY*** Stel de scanprioriteit in op /Low, Auto, High/ (zie Geavanceerde instellingen / Scans)
- ***/SHUTDOWN*** Computer uitschakelen na voltooien van scan
- ***/FORCESHUTDOWN*** Computer geforceerd uitschakelen na voltooien van scan
- ***/ADS*** Alternatieve gegevensstromen scannen (alleen NTFS)

12.5. Scans plannen

Met **AVG 9 Internet Security** kunt u scans op verzoek uitvoeren (bijvoorbeeld als u vermoedt dat uw computer geïnfecteerd is geraakt) of volgens schema. Het is met nadruk raadzaam om de scans op basis van een 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.

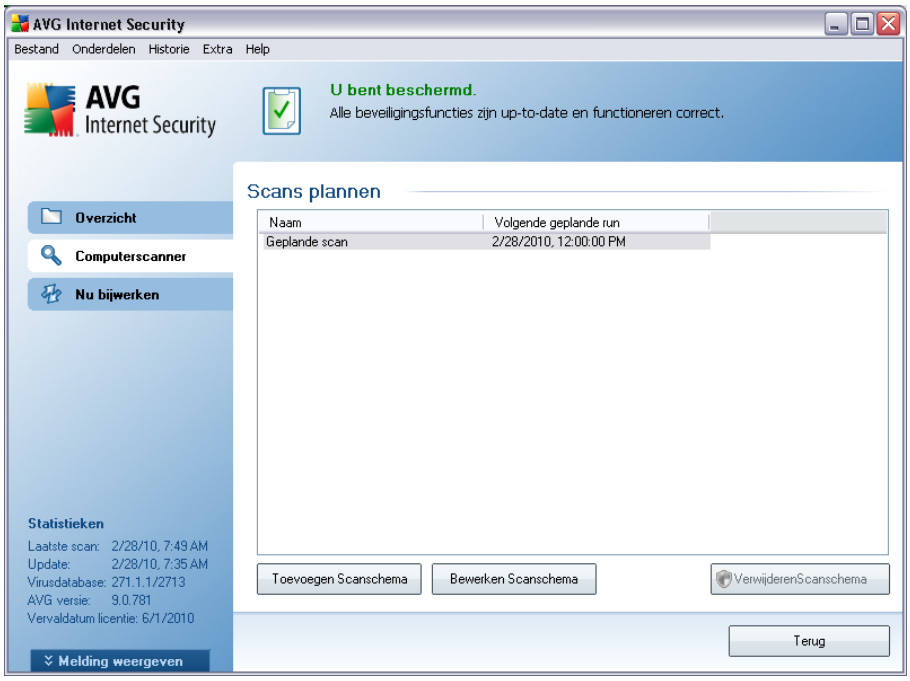
Minimaal voert u ***De hele computer scannen*** regelmatig uit, minstens één maal per week. Als het echter mogelijk is, is het verstandig om de hele computer dagelijks te scannen - zoals ook is ingesteld in de standaardconfiguratie voor scanschema's.Als de computer altijd "aan staat", kunt u de scans 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.

Open het dialoogvenster AVG scaninterface en geef instellingen op in het onderste deel van het dialoogvenster ***Scans plannen*** als u nieuwe scanschema's wilt maken:



Scans plannen

Klik op het pictogram in het gedeelte ***Scans plannen*** om een nieuw dialoogvenster ***Scans plannen*** te openen met een lijst van alle huidige geplande scans:



U kunt scans bewerken/toevoegen met de volgende knoppen:

- ***Scanschema toevoegen*** - als u op deze knop klikt, wordt het dialoogvenster ***Instellingen voor geplande scan*** geopend met het tabblad ***Schema-instellingen***. In dat dialoogvenster kunt u de instellingen opgeven voor de nieuwe scan.

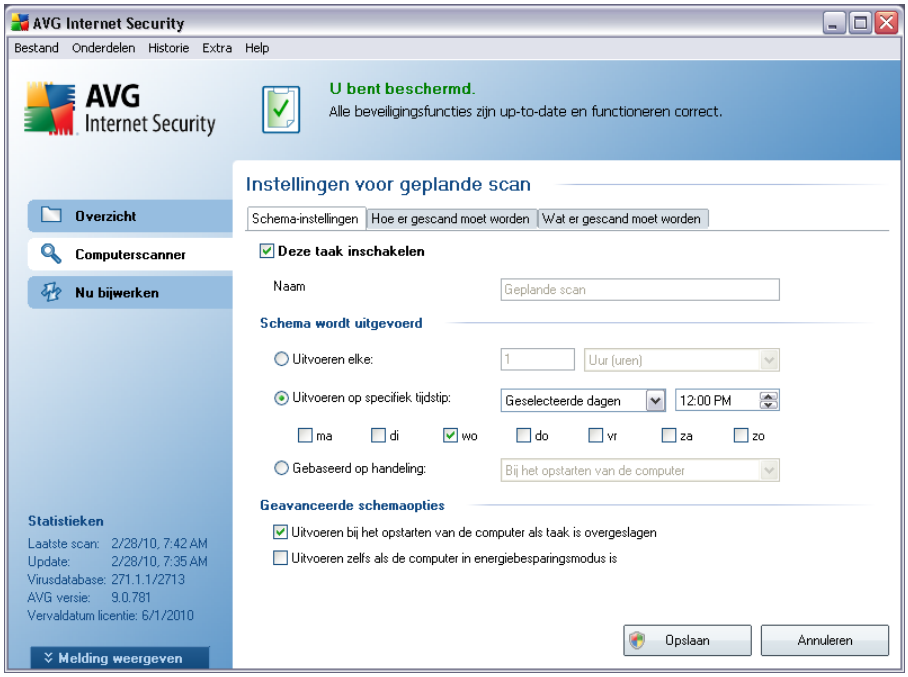
- ***Scanschema bewerken*** - deze knop is alleen actief als u eerst een bestaande scan uit de lijst met geplande scans hebt geselecteerd. In dat geval wordt de knop actief en kunt u erop klikken om het dialoogvenster ***Instellingen voor geplande scan*** te openen, met het tabblad ***Schema-instellingen***. De parameters van de bestaande scan worden weergegeven, u kunt die wijzigen.

- ***Scanschema verwijderen*** - deze knop is eveneens alleen actief als u eerst een bestaande scan uit de lijst met geplande scans hebt geselecteerd. U kunt dat schema dan verwijderen als u op deze knop klikt. U kunt echter alleen uw eigen schema's verwijderen; het vooraf gedefinieerde ***Schema volledige computer scannen*** van de standaardinstellingen kan nooit worden verwijderd.

- ***Terug*** - terugkeren naar de scaninterface van AVG

12.5.1. Schema-instellingen

Als u een nieuwe scan die regelmatig moet worden uitgevoerd, wilt plannen, opent u het dialoogvenster ***Instellingen voor geplande scan*** (*klik op de knop* ***Scanschema toevoegen*** *in het dialoogvenster* ***Scans plannen***). Het dialoogvenster heeft drie tabbladen: ***Schema-instellingen*** - *zie de onderstaande afbeelding*(*(het standaardtabblad dat automatisch wordt weergegeven*), ***Hoe er gescand moet worden*** en ***Wat er gescand moet worden***.



Op het tabblad ***Taakinstellingen*** kunt u eerst het selectievakje ***Deze taak inschakelen*** uitschakelen als u de geplande test tijdelijk niet wilt uitvoeren, en weer inschakelen als de noodzaak daarvoor zich aandient.

Geef vervolgens de scan die u gaat maken en waarvoor u een schema gaat opstellen, een naam. Typ de naam in het tekstvak bij ***Naam***. Probeer korte, maar niettemin veelzeggende namen te gebruiken voor scans zodat u ze achteraf te midden van andere scans kunt herkennen.

Voorbeeld: *het is niet handig om een scan als naam "nieuwe scan" of "mijn scan" te geven, omdat die namen geen aanduiding geven van 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 Bepaalde mappen of bestanden scannen.

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

- ***Schema wordt uitgevoerd*** - geef een tijdsinterval op waarmee de nieuwe geplande scan moet worden uitgevoerd. U kunt deze interval op verschillende manieren definiëren: als steeds terugkerende scan die na verloop van een bepaalde tijd (***Uitvoeren elke ...***) moet worden uitgevoerd, als scan 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 scan moet worden gekoppeld (***Actie bij het opstarten van de computer***).

- ***Geavanceerde schema-opties*** - in deze sectie kunt u bepalen onder welke omstandigheden de scan wel of niet moet worden uitgevoerd als de computer in een energiebesparingsmodus is of helemaal is uitgeschakeld.

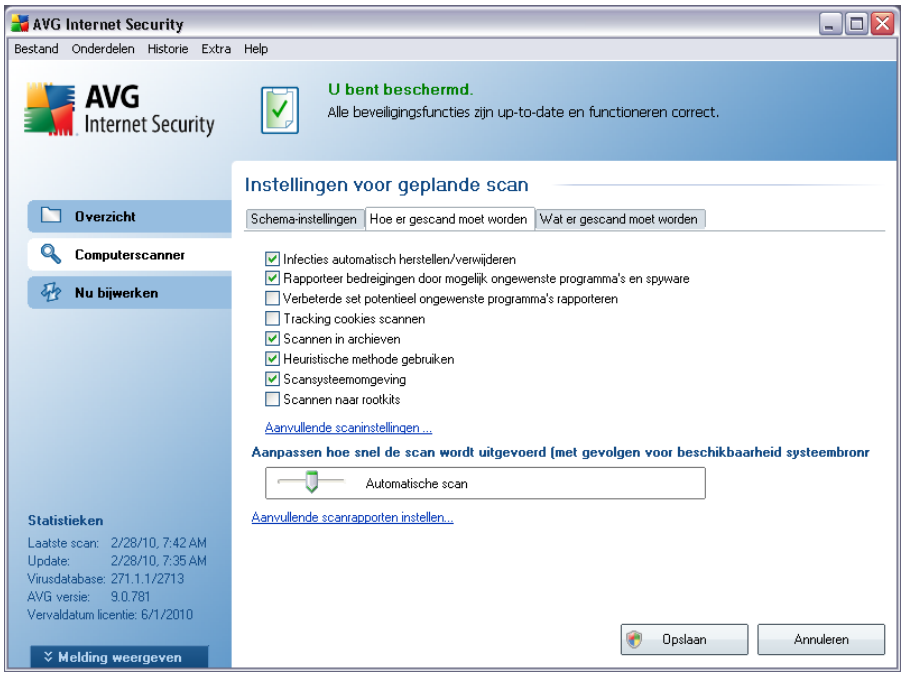
Knoppen in het dialoogvenster Instellingen voor scanschema

Er zijn twee knoppen op alle drie de tabbladen van het dialoogvenster ***Instellingen voor scanschema*** (***Schema-instellingen***, ***Hoe er gescand moet worden*** en ***Wat er gescand moet worden***) en die hebben op alle drie de tabbladen dezelfde functies:

- ***Opslaan*** - opslaan van alle wijzigingen die u hebt uitgevoerd op dit tabblad of een van de twee andere tabbladen van het dialoogvenster, het dialoogvenster sluiten en terugkeren naar het standaarddialoogvenster van de AVG scaninterface. Klik daarom, als u testparameters op alledrie de tabbladen wilt instellen, alleen op de knop om instellingen op te slaan, nadat u al uw wensen hebt gespecificeerd.

- ***Annuleren*** - alle wijzigingen die u hebt aangebracht in instellingen op dit tabblad of één van de twee andere tabbladen van het dialoogvenster, ongedaan maken, het dialoogvenster sluiten en terugkeren naar het standaarddialoogvenster van de AVG scaninterface.

12.5.2. Hoe er gescand moet worden



Op het tabblad ***Hoe er gescand moet worden*** staat een lijst met scanparameters die kunnen worden in- en uitgeschakeld. Standaard zijn de meeste parameters ingeschakeld en wordt de desbetreffende functionaliteit 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:

- ***Infecties automatisch herstellen/verwijderen*** - (*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 hersteld kan worden, of als u besluit deze optie uit te schakelen, wordt u bij detectie van een virus gewaarschuwd en zult u op dat moment moeten besluiten wat u wilt doen met de gedetecteerde infectie. Het is raadzaam het geïnfecteerde bestand te verplaatsen naar de ***Quarantaine***.

- ***Bedreigingen door mogelijk ongewenste programma's en spyware rapporteren*** - (*standaard ingeschakeld*): schakel dit selectievakje in om de ***Anti-Spyware***-engine te activeren en naar spyware en virussen te scannen. Spyware behoort tot een twijfelachtige categorie malware en vormt gewoonlijk een veiligheidsrisico, maar sommige van deze programma's kunnen ook met opzet worden geïnstalleerd. Het is raadzaam deze functie niet uit te schakelen, omdat het de bescherming van uw computer vergroot

- ***Uitgebreide sets van mogelijk ongewenste programma's rapporteren*** - als de vorige optie is geactiveerd, kunt u ook dit selectievakje inschakelen om uitgebreide pakketten van spyware te detecteren: programma's waar op zich niets aan mankeert als u ze direct van de fabrikant krijgt, maar die wel in een later stadium voor kwaadaardige praktijken kunnen worden misbruikt. 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.

- ***Tracking cookies scannen***- (*standaard ingeschakeld*): deze parameter van het onderdeel ***Anti-Spyware*** 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 binnen archieven*** - (*standaard ingeschakeld*): deze parameter bepaalt of bij het scannen alle bestanden moeten worden gecontroleerd, ook als die op de een of andere manier zijn gecomprimeerd, bijv. ZIP, RAR, ...

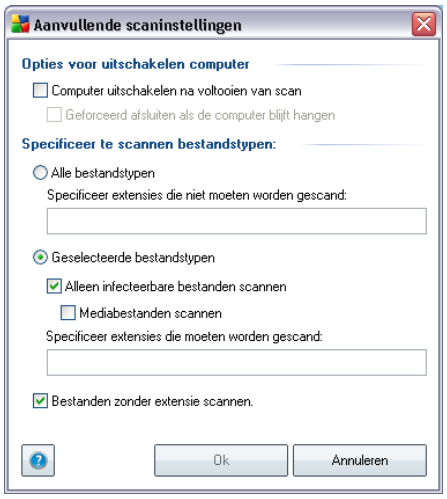
- ***Heuristische methode gebruiken***- (*standaard ingeschakeld*): heuristische analyse (*dynamische emulatie van de instructies van het gescande object in een virtuele computeromgeving*) wordt gebruikt als één van de methoden voor virusdetectie als de parameter is ingeschakeld;

- ***Systeemgebieden scannen*** - (*standaard ingeschakeld*): als de parameter is ingeschakeld worden ook de systeemgebieden gescand;

- ***Scannen naar rootkits*** - schakel dit selectievakje in als u rootkitdetectie wilt opnemen in uw scan van de hele computer. Rootkitdetectie is afzonderlijk beschikbaar in het onderdeel ***Anti-Rootkit;***

U kunt de scanconfiguratie als volgt wijzigen:

- ***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 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***).

- ***Specificeer te scannen bestandstypen*** - geef op wat u precies wilt scannen:

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

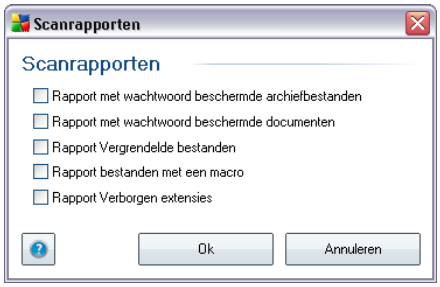
  - ***Geselecteerde bestandstypen*** - u kunt opgeven dat u alleen bestanden wilt scannen die mogelijk geïnfecteerd kunnen worden (*bestanden die niet geïnfecteerd kunnen worden, worden niet gescand, bijvoorbeeld bepaalde niet-opgemaakte tekstbestanden, of andere bestanden die niet uitvoerbaar zijn*), inclusief mediabestanden (*videobestanden, audiobestanden - als u deze optie niet inschakelt, reduceert 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 aan de hand 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 uitermate verdacht en dienen altijd te worden gescand.

- ***Prioriteit scanproces*** - met de schuifbalk kunt u de prioriteit voor het scanproces wijzigen. Standaard is de prioriteit ingesteld op gemiddeld (*Automatische scan*), waarbij de snelheid van het scanproces en het gebruik van systeembronnen (o.a. het werkgeheugen van uw computer) optimaal op elkaar zijn afgesteld. 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 geopend, ***Scanrapporten***, waarin u kunt aangeven wat voor soort resultaten moeten worden gerapporteerd:



Opmerking: *Standaard is de scanconfiguratie ingesteld op optimale prestaties. Het is raadzaam de vooraf ingestelde configuratie aan te houden, tenzij u een goede reden hebt om de scaninstellingen te wijzigen. Alleen ervaren gebruikers dienen wijzigingen aan te brengen in de configuratie. Zie het dialoogvenster* ***Geavanceerde instellingen*** *dat u kunt openen via* ***Bestand/Geavanceerde instellingen*** *in het systeemmenu voor meer opties voor de scanconfiguratie.*

Knoppen

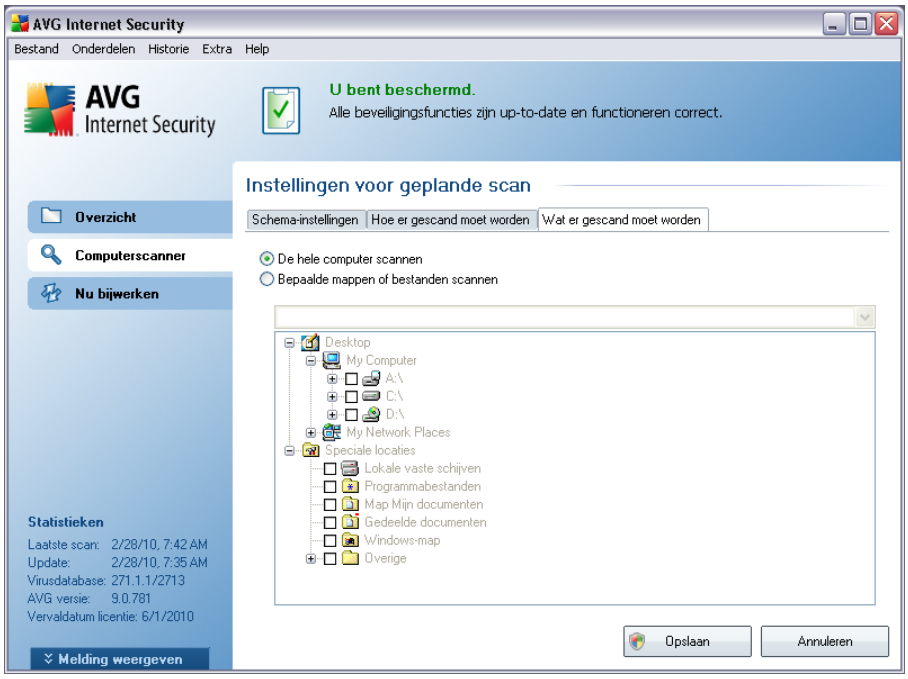
Er zijn twee knoppen op alle drie de tabbladen van het dialoogvenster ***Instellingen voor scanschema*** (***Schema-instellingen***, ***Hoe er gescand moet worden*** en ***Wat er gescand moet worden***) en die hebben op alle drie de tabbladen dezelfde functies:

- ***Opslaan*** - opslaan van alle wijzigingen die u hebt uitgevoerd op dit tabblad of een van de twee andere tabbladen van het dialoogvenster, het dialoogvenster sluiten en terugkeren naar het standaarddialoogvenster van de AVG

scaninterface. Klik daarom, als u testparameters op alledrie de tabbladen wilt instellen, alleen op de knop om instellingen op te slaan, nadat u al uw wensen hebt gespecificeerd.

- ***Annuleren*** - alle wijzigingen die u hebt aangebracht in instellingen op dit tabblad of één van de twee andere tabbladen van het dialoogvenster, ongedaan maken, het dialoogvenster sluiten en terugkeren naar het standaarddialoogvenster van de AVG scaninterface.

12.5.3. Wat er gescand moet worden



Op het tabblad ***Wat er gescand moet worden*** kunt u opgeven welke scan moet worden uitgevoerd: een scan van de hele computer of een scan van specifieke 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 (*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 desbetreffende vakken aan te kruisen. 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. Ook kunt u het volledige pad naar de gewenste map 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 desbetreffende selectievakje hebt ingeschakeld.

- ***Lokale vaste schijven*** - alle vaste schijven van uw computer
- ***Programmabestanden*** - C:\Program Files\
- ***Map Mijn documenten*** - C:\Documents and Settings\Gebruiker\Mijn documenten\
- ***Gedeelde documenten*** - C:\Documents and Settings\All Users\Gedeelde documenten\
- ***Map Windows*** - C:\Windows\
- ***Overig***
  - *Systeemstation* - de vaste schijf waarop het besturingssysteem is geïnstalleerd (meestal C:)
  - *Systeemmap* - Windows/System32
  - *Map voor tijdelijke bestanden* - Documents and Settings/Gebruiker/Local Settings/Temp
  - *Tijdelijke internetbestanden* - Documents and Settings/Gebruiker/Local Settings/Temporary Internet Files

Knoppen in het dialoogvenster Instellingen voor scanschema

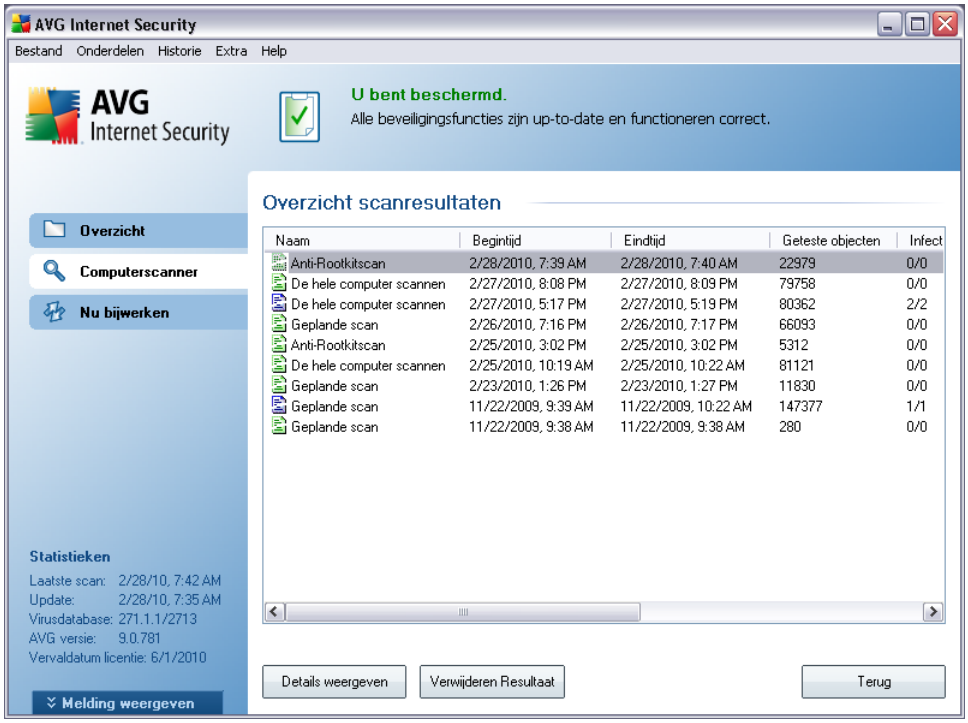
Er zijn twee knoppen op alle drie de tabbladen van het dialoogvenster ***Instellingen voor scanschema*** (***Schema-instellingen***, ***Hoe er gescand moet worden*** en ***Wat er gescand moet worden***) en die hebben op alle drie de tabbladen dezelfde functies:

- ***Opslaan*** - opslaan van alle wijzigingen die u hebt uitgevoerd op dit tabblad of een van de twee andere tabbladen van het dialoogvenster, het dialoogvenster sluiten en terugkeren naar het standaarddialoogvenster van de AVG scaninterface. Klik daarom, als u testparameters op alledrie de tabbladen wilt instellen, alleen op de knop om instellingen op te slaan, nadat u al uw wensen

hebt gespecificeerd.

- ***Annuleren*** - alle wijzigingen die u hebt aangebracht in instellingen op dit tabblad of één van de twee andere tabbladen van het dialoogvenster, ongedaan maken, het dialoogvenster sluiten en terugkeren naar het standaarddialoogvenster van de AVG scaninterface.

12.6. Overzicht scanresultaten



U kunt het dialoogvenster ***Overzicht scanresultaten*** openen als u in de AVG scaninterface op de knop ***Scanhistorie***klikt. In het dialoogvenster staat een lijst met 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
- ***Spyware*** - de hoeveelheid spyware die is gedetecteerd/verwijderd

- ***Waarschuwingen*** - aantal gedetecteerde verdachte objecten
- ***Waarschuwingen*** - aantal gedetecteerde rootkits
  - ***Informatie scanlogboek*** - informatie over het scanverloop en -resultaat (gewoonlijk bij het voltooien of afbreken)

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

- ***Terug*** - terug naar het standaard dialoogvenster van de AVG scaninterface

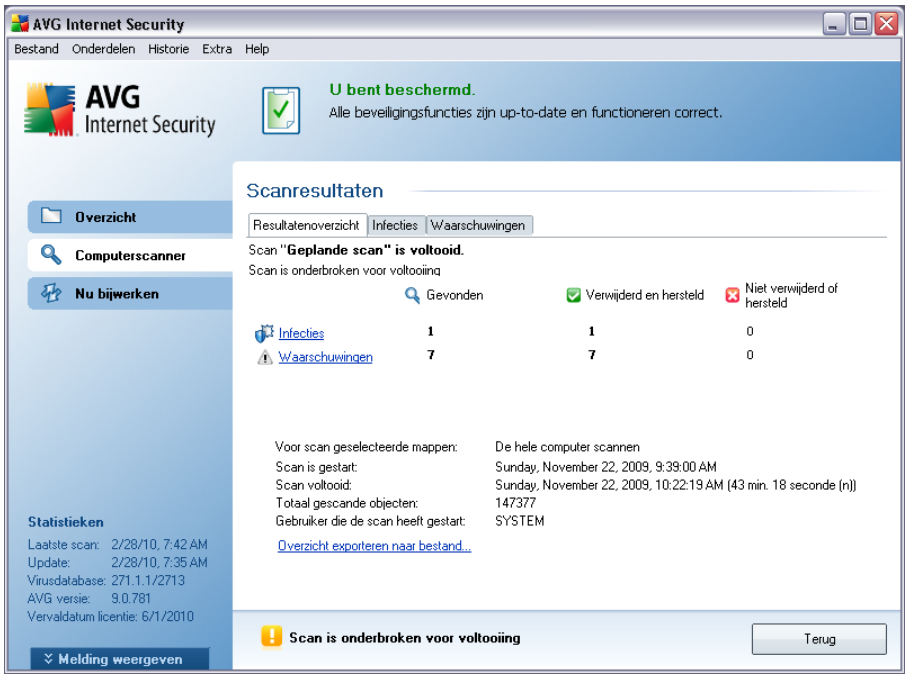
12.7. Details scanresultaten

Als in het dialoogvenster ***Overzicht scanresultaten*** een bepaalde scan is geselecteerd, kunt u op de knop ***Details weergeven*** klikken om het dialoogvenster ***Scan resultaten*** te openen met gedetailleerde informatie over het verloop en de resultaten van de geselecteerde scan.

Het dialoogvenster heeft bovendien een aantal tabbladen:

- ***Resultatenoverzicht*** - dit tabblad wordt steeds weergegeven en bevat statistische gegevens over de voortgang van het scanproces
- ***Infecties*** - dit tabblad wordt alleen weergegeven als een virusinfectie is gedetecteerd tijdens het scannen
- ***Spyware*** - dit tabblad wordt alleen weergegeven als spyware is gedetecteerd tijdens het scannen
- ***Waarschuwingen*** - deze tab wordt bijvoorbeeld weergegeven als er cookies zijn gedetecteerd tijdens het scannen
- ***Rootkits*** - dit tabblad wordt alleen weergegeven als er rootkits zijn gedetecteerd tijdens het scannen
- ***Informatie*** **-** dit tabblad wordt alleen weergegeven als er potentiële gevaren zijn gedetecteerd die niet in de bovenstaande categorieën kunnen worden ondergebracht; in dat geval staat er op het tabbblad een waarschuwing met betrekking tot de vondst. U vindt hier ook informatie over objecten die niet konden worden gescand (bijvoorbeeld archieven die met een wachtwoord zijn beveiligd).

12.7.1. Tabblad Overzicht resultaten



Op het tabblad ***Scanresultaten*** staat gedetailleerd cijfermateriaal met informatie over:

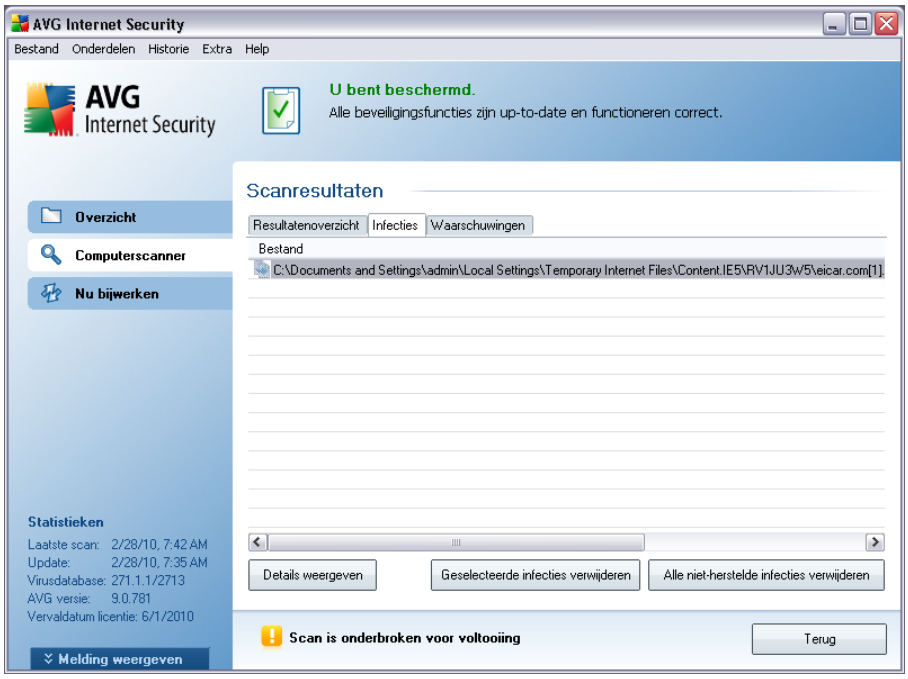
- gedetecteerde virusinfecties / spyware
- verwijderde virusinfecties / spyware
- de hoeveelheid virusinfecties / spyware die niet kan worden verwijderd of hersteld

Bovendien staat er informatie over de datum en het precieze tijdstip waarop de scan is uitgevoerd, het totale aantal gescande objecten, de duur van de scan en het aantal fouten dat tijdens het scannen is opgetreden.

Knoppen

Dit dialoogvenster heeft slechts één knop. Als u op de knop ***Sluiten*** klikt, keert u terug naar het dialoogvenster ***Overzicht scanresultaten***.

12.7.2. Tabblad Infecties



Het Tabblad ***Infecties*** wordt alleen weergegeven in het dialoogvenster ***Scanresultaten*** als tijdens het scannen een virusinfectie is gedetecteerd. Het tabblad is onderverdeeld in drie secties met de volgende informatie:

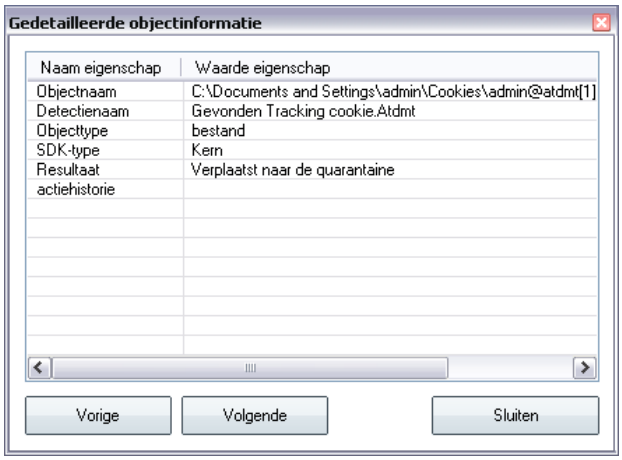
- ***Bestand*** - het volledige pad naar de oorspronkelijke locatie van het geïnfecteerde object
- ***Infecties*** - de naam van het gedetecteerde virus (*Raadpleeg de online Virusencyclopedie voor meer informatie over specifieke virussen*)
- ***Resultaat*** - De huidige status van het geïnfecteerde object dat tijdens het scannen is gedetecteerd:
    - ***Geïnfecteerd*** - het geïnfecteerde object is gedetecteerd, maar niet van de oorspronkelijke locatie verwijderd (*bijvoorbeeld omdat u de functie voor automatisch herstel hebt uitgeschakeldbij bepaalde scaninstellingen*)
    - ***Hersteld*** - het geïnfecteerde object is automatisch hersteld en niet van de oorspronkelijke locatie verwijderd

- ***Verplaatst naar de quarantaine*** - het geïnfecteerde object is verplaatst naar de ***quarantaine***
- ***Verwijderd*** - het geïnfecteerde object is verwijderd
- ***Toegevoegd aan de PUP-uitzonderingen*** - er is vastgesteld dat het gevonden object tot de uitzonderingen behoort en het object is toegevoegd aan de lijst met PUP-uitzonderingen (*geconfigureerd bij **PUP-uitzonderingen** in het dialoogvenster Geavanceerde instellingen*)
- ***Vergrendeld bestand - niet getest*** - het object is vergrendeld en daarom kan AVG het niet scannen
- ***Mogelijk gevaarlijk object*** - het object is gedetecteerd als mogelijk gevaarlijk, maar niet geïnfecteerd (*het kan bijvoorbeeld macro's bevatten*); de informatie moet worden opgevat als waarschuwing
- ***Herstart vereist voor het voltooien van bewerking*** - het geïnfecteerde object kan niet worden verwijderd, voor volledig verwijderen is een herstart van de computer noodzakelijk

Knoppen

Het dialoogvenster heeft drie knoppen:

- ***Details weergeven*** - als u op de knop klikt, wordt een nieuw dialoogvenster ***Details scanresultaten geopend***:



In dat dialoogvenster staat informatie over de locatie van het gedetecteerde geïnfecteerde object (***Naam eigenschap***). Gebruik de knoppen ***Vorige*** / ***Volgende*** om informatie te bekijken over specifieke resultaten. Met de knop ***Sluiten***sluit u het dialoogvenster weer.

- ***Geselecteerde infecties verwijderen*** - klik op deze knop om het geselecteerde object te verplaatsen naar de ***Quarantaine***
- ***Alle niet-herstelde infecties verwijderen*** - als u op deze knop klikt, worden alle objecten verwijderd die niet kunnen worden hersteld of verplaatst naar de ***Quarantaine***
- ***Sluiten*** - het dialoogvenster wordt gesloten en u keert terug naar het dialoogvenster ***Overzicht scanresultaten***

12.7.3. Tabblad Spyware

Het Tabblad ***Spyware*** wordt alleen weergegeven in het dialoogvenster ***Scanresultaten*** als tijdens het scannen een spyware is gedetecteerd. Het tabblad is onderverdeeld in drie secties met de volgende informatie:

- ***Bestand*** - het volledige pad naar de oorspronkelijke locatie van het geïnfecteerde object
- ***Infecties*** - de naam van de gedetecteerde spyware (*Raadpleeg de online **Virusencyclopedie** voor meer informatie over specifieke virussen*)
- ***Resultaat*** - De huidige status van het object dat tijdens het scannen is gedetecteerd:
  - ***Geïnfecteerd*** - het geïnfecteerde object is gedetecteerd, maar niet van de oorspronkelijke locatie verwijderd (bijvoorbeeld omdat u de functie voor automatisch herstel hebt uitgeschakeld bij bepaalde scaninstellingen)
  - ***Hersteld*** - het geïnfecteerde object is automatisch hersteld en niet van de oorspronkelijke locatie verwijderd
  - ***Verplaatst naar de quarantaine*** - het geïnfecteerde object is verplaatst naar de ***quarantaine***
  - ***Verwijderd*** - het geïnfecteerde object is verwijderd
  - ***Toegevoegd aan de PUP-uitzonderingen*** - er is vastgesteld dat het gevonden object tot de uitzonderingen behoort en het object is

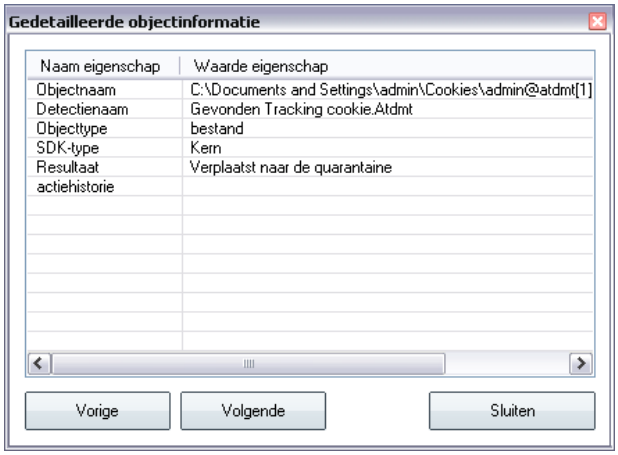
toegevoegd aan de lijst met PUP-uitzonderingen (*geconfigureerd bij **PUP-uitzonderingen** in het dialoogvenster Geavanceerde instellingen*)

- ***Vergrendeld bestand - niet getest*** - het object is vergrendeld en daarom kan AVG het niet scannen
- ***Potentieel gevaarlijk object*** - het object is gedetecteerd als potentieel gevaarlijk, maar niet geïnfecteerd (het kan bijvoorbeeld macro's bevatten); de informatie moet worden opgevat als waarschuwing
- ***Herstart vereist voor het voltooien van bewerking*** - het geïnfecteerde object kan niet worden verwijderd, voor volledig verwijderen is een herstart van de computer noodzakelijk

Knoppen

Het dialoogvenster heeft drie knoppen:

- ***Details weergeven*** - als u op de knop klikt, wordt een nieuw dialoogvenster ***Details scanresultaten*** geopend:



In dat dialoogvenster staat informatie over de locatie van het gedetecteerde geïnfecteerde object (***Naam eigenschap***). Gebruik de knoppen ***Vorige*** / ***Volgende*** om informatie te bekijken over specifieke resultaten. Met de knop ***Sluiten***sluit u het dialoogvenster weer.

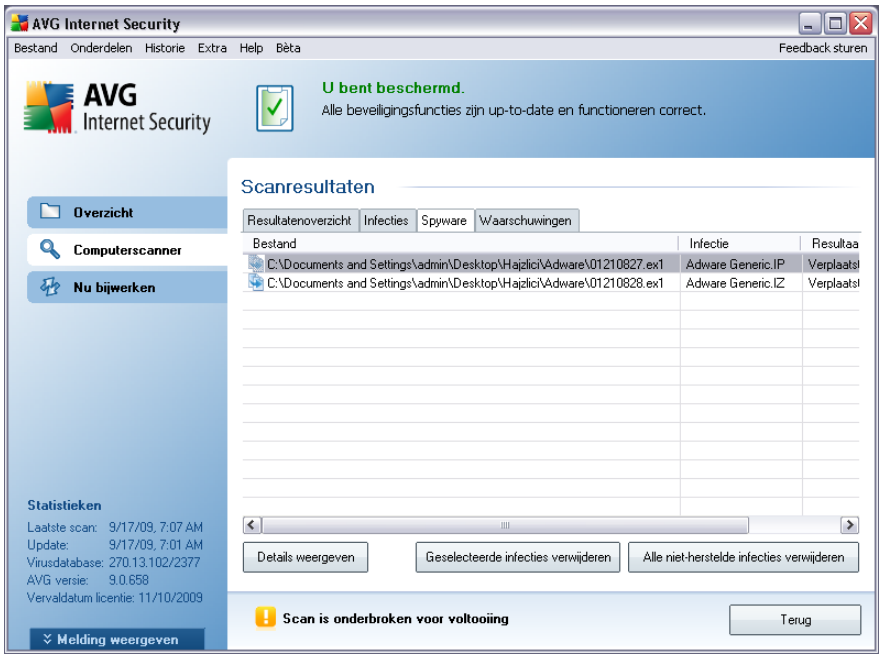
- ***Geselecteerde infecties verwijderen*** - klik op deze knop om het geselecteerde object te verplaatsen naar de ***Quarantaine***

- ***Alle niet-herstelde infecties verwijderen*** - als u op deze knop klikt, worden alle objecten verwijderd die niet kunnen worden hersteld of verplaatst naar de ***Quarantaine***

- ***Sluiten*** - het dialoogvenster wordt gesloten en u keert terug naar het dialoogvenster ***Overzicht scanresultaten***

12.7.4. Tabblad Waarschuwingen

Op het tabblad ***Waarschuwingen*** staat informatie over "verdachte" objecten (*meestal bestanden*) die tijdens het scannen zijn gedetecteerd. Als ze worden gedetecteerd door ***Resident Shield*** worden deze bestanden geblokkeerd zodat ze niet meer toegankelijk zijn. Voorbeelden van dit soort objecten zijn: verborgen bestanden, cookies, verdachte registersleutels, met een wachtwoord beschermde documenten of archiefbestanden, enz.Dergelijke bestanden vormen geen directe bedreiging voor uw computer of beveiliging. Informatie over deze bestanden is over het algemeen handig in geval er adware of spyware op uw computer wordt gedetecteerd. Als er alleen Waarschuwingen in een AVG-test worden gedetecteerd, is geen verdere actie nodig.



Dit is een korte beschrijving van de meest algemene voorbeelden van dergelijke objecten:

- ***Verborgen bestanden*** - de verborgen bestanden zijn standaard niet zichtbaar in Windows, en sommige virussen of andere bedreigingen kunnen detectie

proberen te vermijden door hun bestanden op te slaan met dit kenmerk. Als AVG een verborgen bestand rapporteert dat u verdacht of kwaadaardig voorkomt, kunt u het verplaatsen naar de ***AVG Quarantaine***.

- ***Cookies*** - cookies zijn tekstbestanden die worden gebruikt door websites voor het opslaan van gebruikersspecifieke informatie, die later wordt gebruikt voor het laden van aangepaste websitelayouts, het vooraf invullen van gebruikersnamen, etc.

- ***Verdachte registersleutels*** - sommige malware slaat zijn informatie op in het Windows register, om ervoor te zorgen dat deze informatie wordt geladen na het opstarten of om het effect ervan op het besturingssysteem te vergroten.

12.7.5. Tabblad Rootkits

Op het tabblad ***Rootkits*** staat informatie over rootkits die zijn gedetecteerd bij het scannen als u de ***Anti-Rootkitscan*** hebt gestart, of handmatig de optie voor het scannen op rootkits heb toegevoegd aan ***Volledige computer scannen*** (*deze optie is standaard uitgeschakeld*).

Een ***rootkit*** is een programma dat is ontwikkeld om de controle over een computersysteem over te nemen zonder toestemming van de eigenaren en rechtmatige beheerders van het systeem. Toegang tot de hardware is zelden vereist omdat een rootkit is bedoeld om de controle over het besturingssysteem dat op de hardware draait, over te nemen. Gewoonlijk proberen rootkits hun aanwezigheid te verbergen door het ondermijnen of ontwijken van de standaard beveiligingsmechanismen van het besturingssysteem. Vaak zijn het bovendien Trojaanse paarden die gebruikers in de waan laten dat ze veilig met hun systeem kunnen werken. De technieken die worden gebruikt om dit te bereiken omvatten bijvoorbeeld het voor bewakingsprogramma's verbergen van processen die worden uitgevoerd, of het verbergen van bestanden of systeemgegevens voor het besturingssysteem.

De structuur van dit tabblad is in principe hetzelfde als die van het tabblad ***Infecties*** of het tabblad ***Spyware***.

12.7.6. Tabblad Informatie

Op het tabblad ***Informatie*** staan gegevens over objecten die niet kunnen worden ondergebracht bij infecties, spyware, e.d. Er kan niet worden vastgesteld dat ze gevaarlijk zijn, maar het is wel belangrijk er aandacht aan te besteden. AVG Scan kan bestanden detecteren die wellicht niet zijn geïnfecteerd, maar wel verdacht zijn. Die bestanden worden gerapporteerd als ***Waarschuwing*** of als ***Informatie***.

Het ***bedreigingsniveau*** kan om de volgende redenen worden gerapporteerd:

- ***Runtime-gecomprimeerd*** - het bestand is gecomprimeerd met een van de minder gangbare runtime-compressieprogramma's, wat kan duiden op een poging een scan van het bestand te ontwijken. Niet elk incident dat als zodanig wordt gerapporteerd, betreft ook daadwerkelijk een virus.

- ***Runtime-gecomprimeerd recursief*** - vergelijkbaar met bovenstaande, maar komt minder voor bij gangbare software. Dergelijke bestanden zijn verdacht en verwijdering of verzending voor analyse moet worden overwogen.

- ***Met een wachtwoord beschermde documenten of archieven*** - bestanden die zijn beveiligd met een wachtwoord kunnen door AVG niet worden gescand (*en in het algemeen niet met anti-malwareprogramma's*).

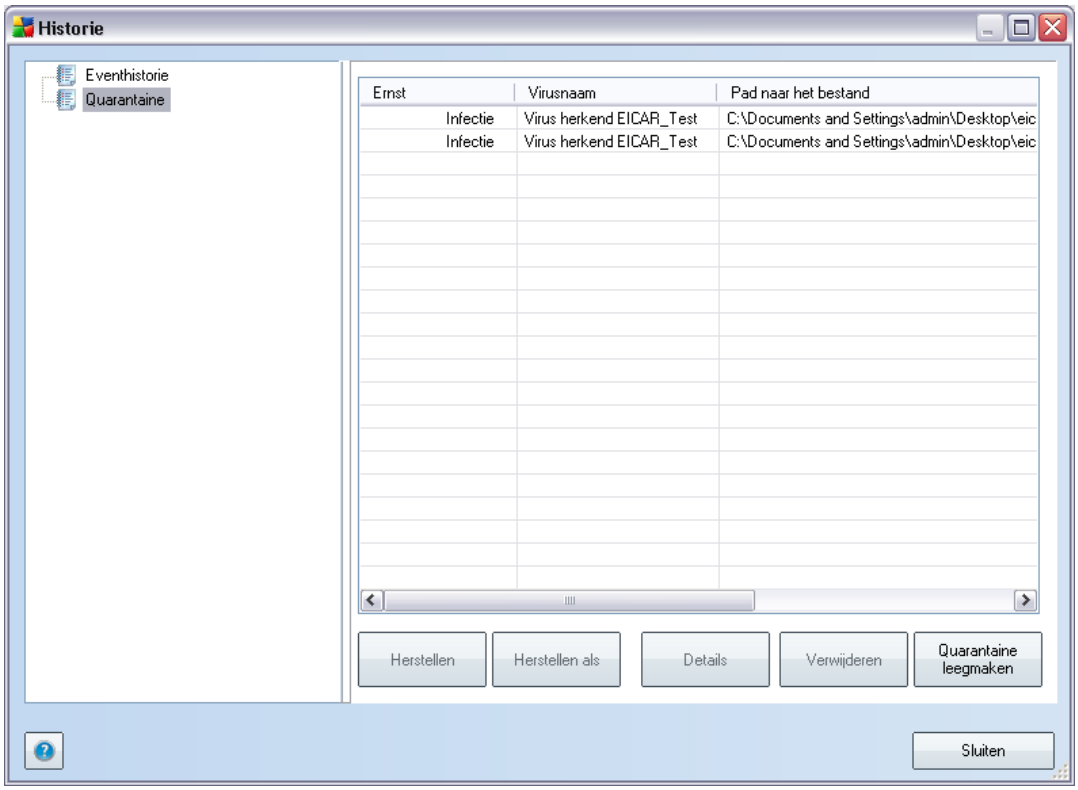
- ***Document met macro's*** - het gerapporteerde document bevat macro's die kwaadaardig kunnen zijn.

- ***Verborgen extensies*** - bestanden met verborgen extensies kunnen op het oog bijvoorbeeld afbeeldingsbestanden lijken te zijn, terwijl het in werkelijkheid uitvoerbare bestanden zijn (*bijvoorbeeld picture.jpg.exe*). De tweede extensie is in Windows standaard niet zichtbaar en AVG rapporteert dergelijke bestanden om te voorkomen dat ze per ongeluk worden geopend.

- ***Onjuist bestandspad*** - als een belangrijk systeembestand wordt uitgevoerd vanuit een andere map dan de standaardmap (*het bestand winlogon.exe wordt bijvoorbeeld uitgevoerd vanuit een andere map dan de map Windows*), wordt dat door AVG gemeld. In sommige gevallen gebruiken virussen de namen van standaardprocessen om minder opvallend aanwezig te zijn in het systeem.

- ***Vergrendeld bestand*** - het gerapporteerde bestand is vergrendeld en kan dus niet worden gescand door AVG. Dat betekent meestal dat een bestand voortdurend wordt gebruikt door het systeem (*bijvoorbeeld het wisselbestand*).

12.8. Quarantaine



Quarantaine voorziet in een veilige omgeving voor het beheren van verdachte of geïnfecteerde objecten die tijdens AVG-tests 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 desbetreffende bestand opsturen voor analyse of het terugzetten naar de oorspronkelijke locatie.

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

- ***Ernst*** - als u besluit om het onderdeel ***Identity Protection*** in **AVG 9 Internet Security** te installeren, wordt er in dit gedeelte een grafische indicatie voor

het bedreigingsniveau van het desbetreffende resultaat weergegeven op een schaal met vier niveaus, van ongevaarlijk (■□□□) tot erg gevaarlijk (■■■■), alsmede informatie over het type infectie (*gebaseerd op het infectieniveau - alle objecten in de lijst zijn of zijn mogelijk geïnfecteerd*)

- ***Virusnaam*** - de naam van het gedetecteerde virus, zoals dat is geregistreerd in de Virusencyclopedie (online)
- ***Pad naar het bestand*** - het volledige pad naar de oorspronkelijke locatie van het gedetecteerde geïnfecteerde bestand
- ***Oorspronkelijke objectnaam*** - alle gedetecteerde objecten die worden weergegeven in het diagram zijn gelabeled met de standaardnaam die werd gegeven door AVG tijdens de scanprocedure. Als het object een specifieke, oorspronkelijke naam had die bekend is, (*bijvoorbeeld een naam van een e-mailbijlage die geen relatie heeft tot de feitelijke inhoud van de bijlage*), wordt de naam weergegeven in deze kolom.
- ***Datum van opslaan*** - datum en tijdstip van detectie van het verdachte bestand en verplaatsing naar de ***Quarantaine***

Knoppen

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

- ***Herstellen*** - Het geïnfecteerde bestand wordt teruggeplaatst op de oorspronkelijke locatie
- ***Herstellen als*** - als u besluit om het gedetecteerde, geïnfecteerde object te verplaatsen van de ***Quarantaine*** naar een geselecteerde map, gebruikt u deze knop. Het verdachte en gedetecteerde object wordt opgeslagen met zijn oorspronkelijke naam. Als de oorspronkelijke naam niet bekend is, wordt de standaardnaam gebruikt.
- ***Details*** - deze knop is alleen van toepassing op bedreigingen die zijn gedetecteerd door ***Identity Protection***. Als u erop klikt, wordt een samenvatting weergegeven van de details van de bedreiging (*welke bestanden/processen zijn aangetast, eigenschappen van het proces, enz.*). Bij alle andere items is de knop grijs en niet actief!
- ***Verwijderen*** - Het geïnfecteerde bestand wordt volledig en onherroepelijk uit de ***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).

13. AVG Updates

Het is van cruciaal belang om uw AVG up-to-date te houden zodat alle nieuw ontdekte virussen zo snel mogelijk gedetecteerd kunnen worden.

Tijdens de installatieprocedure van AVG werd u gevraagd op te geven hoe vaak u uw AVG-product wilt updaten. U hebt de keuze uit ***Om de 4 uur*** of ***Elke dag*** (zie het dialoogvenster ***Regelmatige scans en updates plannen***). Het is raadzaam om minstens eenmaal per dag te controleren of er nieuwe updates zijn, omdat AVG-updates niet volgens een bepaald schema worden uitgebracht, maar in reactie op het aantal bedreigingen en de ernst daarvan. Als u om de 4 uur laat checken op nieuwe updates, bent u er van verzekerd dat **AVG 9 Internet Security** elke dag up-to-date gehouden wordt.

13.1. Updateniveaus

AVG kent drie updateniveaus die u kunt selecteren:

- ***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.

Bij het plannen van een update, kunt u selecteren op welk prioriteitsniveau u wilt downloaden en updates wilt uitvoeren.

Opmerking: *Bij tijdconflicten tussen een geplande programma-update en een geplande scan krijgt het updateproces een hogere prioriteit en zal het scannen worden onderbroken.*

13.2. Soorten updates

Er zijn twee soorten updates te onderscheiden:

- ***Een update op verzoek*** is een onmiddellijke AVG-update die kan worden uitgevoerd zodra de noodzaak zich daartoe voordoet.

- ***Geplande update*** - U kunt in AVG ook een updateplan instellen. De geplande update wordt vervolgens op basis van de ingestelde configuratie periodiek uitgevoerd. Wanneer er op de ingestelde locatie nieuwe updatebestanden beschikbaar zijn, worden deze rechtstreeks van internet of vanuit de

netwerkmap gedownload. Als er geen nieuwe updates beschikbaar zijn, gebeurt er niets.

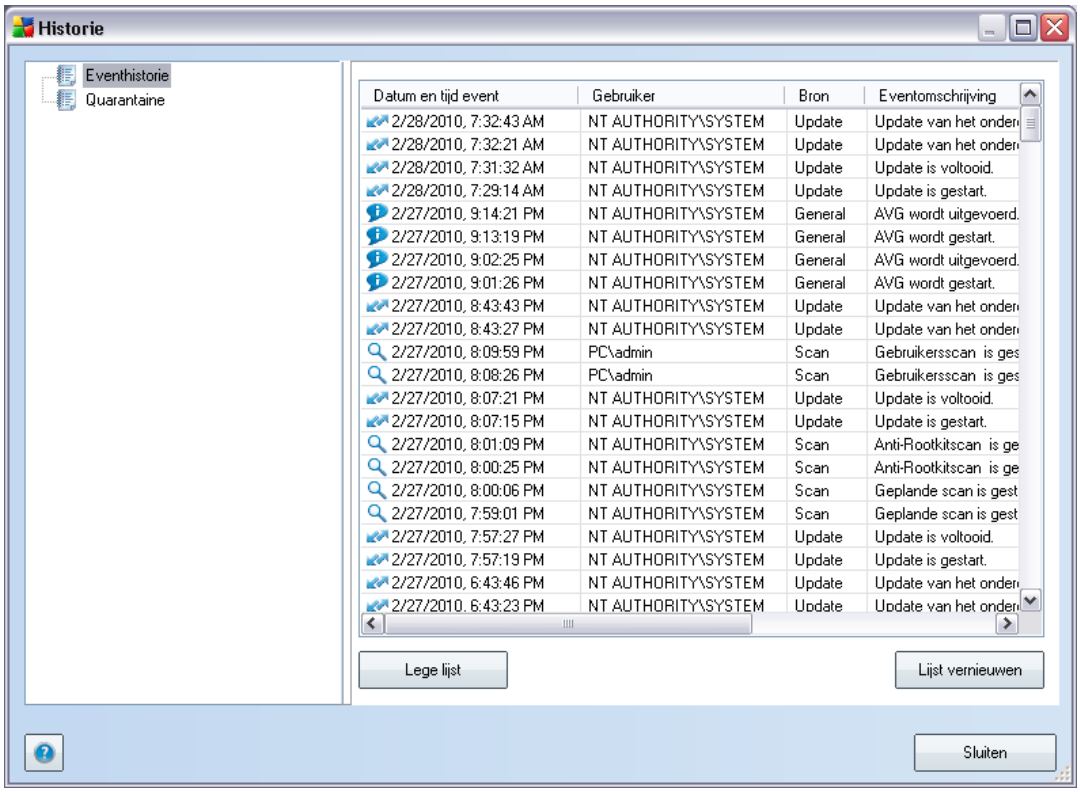
13.3. Updateprocedure

De updateprocedure kan als dat nodig is, onmiddellijk worden uitgevoerd als u op de snelkoppeling ***Nu bijwerken***klikt. De koppeling is altijd actief in alle dialoogvensters van deAVG gebruikersinterface. Het blijft echter raadzaam om regelmatig updates uit te voeren met behulp van het updateschema dat u kunt bewerken in het onderdeel Updatebeheer.

Als u de updateprocedure start, wordt eerst gecontroleerd of er nieuwe updates beschikbaar zijn. Zo ja, dan worden die gedownload en wordt het proces voor het bijwerken op gang gebracht. Tijdens het uitvoeren van de updateprocedure wordt het dialoogvenster ***Update*** geopend dat op grafische wijze de voortgang in beeld brengt en bovendien een overzicht geeft van de relevante statistische parameters (*grootte updatebestand, ontvangen gegevens, downloadsnelheid, verstreken tijd, ...*).

Opmerking*: Voorafgaand aan de start van de AVG-programma-update wordt een systeemherstelpunt gemaakt. Als de updateprocedure faalt en uw besturingssysteem crasht, kunt u uw besturingssysteem altijd herstellen in de oorspronkelijke configuratie vanaf dit punt. Deze optie is toegankelijk via Start / Alle programma's / Accessoires / Systeemprogramma's / Systeemherstel. Het aanbrengen van wijzigingen wordt alleen aanbevolen aan ervaren gebruikers!*

14. Gebeurtenishistorie



U kunt het dialoogvenster ***Gebeurtenishistorie*** openen met de systeemmenu-optie ***Historie/Gebeurtenishistorie Logboek***. In het dialoogvenster wordt een overzicht weergegeven van belangrijke gebeurtenissen die tijdens het uitvoeren van **AVG 9 Internet Security** zijn opgetreden. ***Gebeurtenishistorie*** legt de volgende gebeurtenistypen vast:

- Informatie over updates van de AVG-toepassing
- Het begin en einde van een scan, en of de test stopgezet is (inclusief automatisch uitgevoerde tests)
- Gebeurtenissen die verband houden met virusdetectie (door Resident Shield of tijdens scannen), waaronder de detectielocatie
- Andere belangrijke gebeurtenissen

Knoppen

- ***Lijst legen*** - alle items uit de lijst gebeurtenissen verwijderen
- ***Lijst vernieuwen*** - alle items in de lijst gebeurtenissen bijwerken

15. Veelgestelde vragen en technische ondersteuning

Mocht u problemen ondervinden met AVG, op zakelijk of technisch gebied, raadpleeg dan de sectie met ***veelgestelde vragen(FAQ)*** op de website van AVG (http://www.avg.com/).

Vindt u op die manier geen oplossing, neem dan via e-mail contact op met de technische ondersteuningsdienst. Gebruik daarvoor het contactformulier dat u kunt oproepen in het systeemmenu via de optie ***Help / Online Help***.