AVG Anti-Virus 2012

Gebruikershandleiding

Documentrevisie 2012.03 (29.11.2011)

Copyright AVG Technologies CZ, s.r.o. Alle rechten voorbehouden.
Alle overige handelsmerken zijn het eigendom van de respectieve eigenaren.

Dit product maakt gebruik van RSA Data Security, Inc. MD5 Message-Digest-algoritme, Copyright (C) 1991-2, RSA Data Security, Inc. Opgericht in 1991.
Dit product gebruikt code van de C-SaCzech bibliotheek, Copyright © 1996-2001 Jaromir Dolecek (dolecek@ics.muni.cz).
Dit product gebruikt compressiebibliotheek zlib, copyright (c) 1995-2002 Jean-loup Gailly en Mark Adler.
Dit product gebruikt compressiebibliotheek libbzip2, copyright (c) 1996-2002 Julian R. Seward.

Inhoud

1. Inleiding 6

2. AVG-installatievereisten 7

2.1 Ondersteunde besturingssystemen 7
2.2 Minimale en aanbevolen hardwarevereisten 7

3. AVG-installatieprocedure 8

3.1 Welkom 8
3.2 Uw licentie activeren 10
3.3 Type installatie selecteren 11
3.4 Aangepaste opties 12
3.5 De AVG Werkbalk Beveiliging installeren 14
3.6 Installatievoortgang 15
3.7 Installatie voltooid 16

4. Na de installatie 18

4.1 Productregistratie 18
4.2 Toegang tot gebruikersinterface 18
4.3 Volledige computerscan 18
4.4 De EICAR-test 18
4.5 AVG-standaardconfiguratie 19

5. AVG-gebruikersinterface 20

5.1 Systeemmenu 21
5.1.1 Bestand 21
5.1.2 Onderdelen 21
5.1.3 Historie 21
5.1.4 Extra 21
5.1.5 Help 21
5.1.6 Ondersteuning 21
5.2 Info Beveiligingsstatus 28
5.3 Snelkoppelingen 29
5.4 Overzicht van onderdelen 30
5.5 Systeemvakpictogram 32
5.6 AVG-gadget 33

6. AVG-onderdelen 36

AVG Anti-Virus 2012 © 2011 Copyright AVG Technologies CZ, s.r.o. Alle rechten voorbehouden.

6.1 Antivirus 36
6.1.1 Scanprogramma *36*
6.1.2 Residente beveiliging *36*
6.1.3 Beveiliging tegen spyware *36*
6.1.4 Antivirus-interface *36*
6.1.5 Detecties door Resident Shield *36*
6.2 LinkScanner 42
6.2.1 LinkScanner-interface *42*
6.2.2 Detecties door Search-Shield *42*
6.2.3 Detecties door Surf-Shield *42*
6.2.4 Detecties door Online Shield *42*
6.3 E-mailbescherming 48
6.3.1 E-mailscanner *48*
6.3.2 Antispam *48*
6.3.3 E-mailbescherming-interface *48*
6.3.4 Detecties door E-mailbescherming *48*
6.4 Antirootkit 52
6.4.1 Antirootkit-interface *52*
6.5 PC Analyzer 54
6.6 Identity Protection 56
6.6.1 Identiteitsbescherming-interface *56*
6.7 Extern beheer 59

7. Mijn apps 60

7.1 LiveKive 60
7.2 Veiligheid voor het gezin 61
7.3 PC TuneUp 61

8. AVG Werkbalk Beveiliging 63

9. AVG Geavanceerde instellingen 65

9.1 Weergave 65
9.2 Geluiden 68
9.3 Beveiliging door AVG tijdelijk uitschakelen 69
9.4 Anti-Virus 70
9.4.1 Resident Shield *70*
9.4.2 Cacheserver *70*
9.5 E-mailbescherming 76
9.5.1 E-mailscanner *76*

9.6 LinkScanner 85
9.6.1 Instellingen LinkScanner 85
9.6.2 Online Shield 85
9.7 Scans 88
9.7.1 De hele computer scannen 88
9.7.2 Scan van Shell-extensie 88
9.7.3 Mappen of bestanden scannen 88
9.7.4 Scan van verwisselbaar apparaat 88
9.8 Schema's 94
9.8.1 Geplande scan 94
9.8.2 Schema voor definitie-updates 94
9.8.3 Updateschema programma 94
9.9 Update 104
9.9.1 Proxy 104
9.9.2 Inbellen 104
9.9.3 URL 104
9.9.4 Beheer 104
9.10 Antirootkit 111
9.10.1 Uitzonderingen 111
9.11 Identity Protection 112
9.11.1 Identity Protection instellingen 112
9.11.2 Lijst Toegestaan 112
9.12 Mogelijk ongewenste programma's 116
9.13 Quarantaine 119
9.14 Programma voor productverbetering 119
9.15 Foutstatus negeren 122
9.16 Extern beheer 123

10. AVG scannen 125

10.1 Scaninterface 125
10.2 Vooraf ingestelde scans 126
10.2.1 De hele computer scannen 126
10.2.2 Bepaalde mappen of bestanden scannen 126
10.2.3 Antirootkitscan 126
10.3 Scannen in Windows Verkenner 136
10.4 Scannen vanaf opdrachtregel 137
10.4.1 CMD-scanparameters 137
10.5 Scans plannen 140

AVG Anti-Virus 2012 © 2011 Copyright AVG Technologies CZ, s.r.o. Alle rechten voorbehouden.

10.5.1 Schema-instellingen *140*
10.5.2 Hoe er gescand moet worden *140*
10.5.3 Wat er gescand moet worden *140*
10.6 Overzicht scanresultaten 149
10.7 Details scanresultaten 150
10.7.1 Tabblad Overzicht resultaten *150*
10.7.2 Tabblad Infecties *150*
10.7.3 Tabblad Spyware *150*
10.7.4 Tabblad Waarschuwingen *150*
10.7.5 Tabblad Rootkits *150*
10.7.6 Tabblad Informatie *150*
10.8 Quarantaine 158

11. AVG Updates 160

11.1 Update starten 160
11.2 Voortgang van update 160
11.3 Updateniveaus 161

12. Eventhistorie 162

13. Veelgestelde vragen en technische ondersteuning 164

1. Inleiding

Deze gebruikershandleiding bevat uitgebreide informatie over **AVG Anti-Virus 2012**.

AVG Anti-Virus 2012 biedt realtime beveiliging tegen geavanceerde hedendaagse bedreigingen. U kunt zorgeloos chatten, bestanden downloaden en uitwisselen en u kunt games spelen en video's weergeven zonder zorgen of onderbrekingen:

- U kunt bestanden veilig downloaden en delen en u kunt berichten veilig versturen dankzij AVG Online Shield™
- Uw veiligheid op sociale netwerken wordt gewaardborgd door AVG Social Networking Protection
- U kunt dankzij de realtime beveiliging van LinkScanner vol vertrouwen surfen en zoeken

AVG Anti-Virus 2012 © 2011 Copyright AVG Technologies CZ, s.r.o. Alle rechten voorbehouden.

2. AVG-installatievereisten

2.1. Ondersteunde besturingssystemen

AVG Anti-Virus 2012is ontworpen om werkstations met de volgende besturingssystemen te beschermen:

- Windows XP Home Edition SP2
- Windows XP Professional SP2
- Windows XP Professional x64 Edition SP1
- Windows Vista (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 en XP x64. U kunt AVG Anti-Virus 2012 op deze besturingssystemen installeren, maar dan zonder het onderdeel IDP.*

2.2. Minimale en aanbevolen hardwarevereisten

Minimale hardwarevereisten voor **AVG Anti-Virus 2012**:

- Intel Pentium CPU 1,5 GHz
- 512 MB RAM-geheugen
- 950 MB aan vrije vaste schijfruimte (voor installatiedoeleinden)

Aanbevolen hardwarevereisten voor **AVG Anti-Virus 2012**:

- Intel Pentium CPU 1,8 GHz
- 512 MB RAM-geheugen
- 1350 MB aan vrije vaste schijfruimte (voor installatiedoeleinden)

AVG Anti-Virus 2012 © 2011 Copyright AVG Technologies CZ, s.r.o. Alle rechten voorbehouden.

3. AVG-installatieprocedure

Waar kan ik het installatiebestand verkrijgen

Als u **AVG Anti-Virus 2012** op uw computer wilt installeren, moet u over het meest recente installatiebestand beschikken. Het is raadzaam om het installatiebestand te downloaden vanaf de AVG-website (http://www.avg.com/), zodat u er zeker van kunt zijn dat u over de meest recente versie van **AVG Anti-Virus 2012** beschikt. In de sectie ***Help / Downloaden*** vindt u een gestructureerd overzicht van alle installatiebestanden van afzonderlijke AVG-edities.

Als u niet zeker weet welke bestanden u moet downloaden en installeren, kunt u de service ***Product selecteren*** gebruiken die onder op de webpagina wordt weergeven. Nadat u drie eenvoudige vragen hebt beantwoord, bepaalt de service welke bestanden u precies nodig hebt. Druk op de knop ***Doorgaan*** als u een volledige lijst met gedownloade bestanden wilt weergegeven, die is afgestemd op uw persoonlijke behoeften.

Hoe ziet het installatieproces er uit

Als u het installatiebestand hebt gedownload en opgeslagen op uw vaste schijf, kunt u de installatieprocedure starten. De installatie heeft de vorm van een reeks eenvoudige en begrijpelijke dialoogvensters. Elk dialoogvenster bevat een beknopte beschrijving van de afzonderlijke stap van het installatieproces. Vervolgens wordt er een gedetailleerde uitleg van de afzonderlijke dialoogvensters weergegeven:

3.1. Welkom

Het installatieproces start met het dialoogvenster ***Welkom bij het installatieprogramma***:

Selecteer de installatietaal

In dit dialoogvenster kunt u de taal selecteren die voor het installatieproces wordt gebruikt. Klik rechts in de hoek van het dialoogvenster op de keuzelijst, zodat de lijst met talen wordt weergegeven. Selecteer de gewenste taal. Het installatieproces wordt vervolgens voortgezet in de taal die u hebt gekozen.

Let op: u selecteert op dit moment uitsluitend de taal van het installatieproces. De AVG Anti-Virus 2012-toepassing wordt geïnstalleerd in de geselecteerde taal en in de standaardtaal Engels die altijd automatisch wordt geïnstalleerd. Het is echter mogelijk om meerdere talen te installeren en AVG Anti-Virus 2012 in welke van deze talen dan ook te gebruiken. U wordt in een van de volgende installatiedialoogvensters gevraagd om de volledige selectie met betrekking tot alternatieve talen te bevestigen. Dit is in het dialoogvenster Aangepaste opties.

Licentieovereenkomst

Daarnaast bevat het dialoogvenster ***Welkom bij het installatieprogramma*** de volledige tekst van de AVG-licentieovereenkomst. Lees deze tekst zorgvuldig door. Klik op de knop ***Accepteren*** om aan te geven dat u de tekst hebt gelezen, begrepen en geaccepteerd. Als u niet instemt met de licentieverklaring, klikt u op de knop ***Afwijzen***, dan wordt de installatieprocedure meteen afgebroken.

AVG-privacybeleid

Naast de licentieovereenkomst biedt het installatiedialoogvenster tevens de mogelijkheid om meer informatie weer te geven over het AVG-privacybeleid. Links onder in de hoek van het dialoogvenster wordt de koppeling ***AVG Privacybeleid*** weergegeven. Klik op deze koppeling als u de AVG-website (http://www.avg.com/) wilt weergeven. Op deze website wordt de volledige reikwijdte van de principes van het AVG Technologies-privacybeleid beschreven.

Knoppen

Het eerste installatiedialoogvenster bevat slechts twee knoppen:

- ***Accepteren*** - Klik om te bevestigen dat u de licentieovereenkomst hebt gelezen, begrepen en geaccepteerd. De installatie wordt voortgezet en u gaat een stap verder naar het volgende installatiedialoogvenster.
- ***Afwijzen*** - Klik hierop als u de licentieovereenkomst wilt weigeren. Het installatieproces wordt onmiddellijk afgesloten. **AVG Anti-Virus 2012** wordt niet geïnstalleerd.

3.2. Uw licentie activeren

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

Waar vindt u uw licentienummer

Het verkoopnummer wordt weergegeven op de cd-verpakking in de doos van **AVG Anti-Virus 2012**. Het licentienummer staat in de bevestiging die u via e-mail hebt ontvangen na aankoop van **AVG Anti-Virus 2012** 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.

Kopiëren en plakken gebruiken

Gebruik ***kopiëren en plakken*** om uw **AVG Anti-Virus 2012**-licentienummer in het programma te plakken, zodat u er zeker van kunt zijn dat het nummer op de juiste wijze wordt ingevoerd. Ga als volgt te werk:

- Open het e-mailbericht dat uw licentienummer bevat.
- Klik met de linkermuisknop aan het begin van het licentienummer, houd de muisknop ingedrukt, sleep de muiswijzer naar het einde van het nummer en laat vervolgens de knop los. Het nummer moet nu gemarkeerd zijn.
- Druk op de toets ***Ctrl***, houd deze toets ingedrukt en druk vervolgens op ***C***. Hiermee kopieert u het nummer.
- Wijs de positie aan waarop u het gekopieerde nummer wilt plakken en klik op deze positie.

- Druk op de toets ***Ctrl*** houd deze toets ingedrukt en druk vervolgens op ***V***. Hiermee plakt u het nummer op de geselecteerde locatie.

Knoppen

Er zijn drie knoppen beschikbaar, zoals dat ook het geval is binnen de meeste installatiedialoogvensters:

- ***Terug*** – Klik op deze knop als u terug wilt keren naar het vorige installatiedialoogvenster.
- ***Volgende*** – Klik op deze knop als u de installatie wilt voortzetten en als u wilt doorgaan met de volgende stap.
- ***Annuleren*** – Klik op deze knop als u het installatieproces onmiddellijk wilt afsluiten. **AVG Anti-Virus 2012** wordt niet geïnstalleerd.

3.3. Type installatie selecteren

Installatietypen

In het dialoogvenster ***Installatietype selecteren*** kunt u kiezen uit twee soorten installaties: ***Snelle installatie*** en ***Aangepaste installatie***.

Voor het merendeel van de gebruikers wordt de standaardinstelling Snelle installatie aangeraden, waarbij **AVG Anti-Virus 2012** in een automatische modus wordt geïnstalleerd met vooraf door de leverancier ingestelde instellingen. Die configuratie combineert maximale bescherming met een efficiënt gebruik van bronnen. Als het in de toekomst nodig mocht zijn om de configuratie aan te passen, kunt u dat altijd rechtstreeks in de toepassing **AVG Anti-Virus 2012** doen. Als u de optie ***Snelle installatie*** hebt gekozen, klikt u op de knop ***Volgende*** om naar het volgende dialoogvenster De AVG Werkbalk Beveiliging installeren te gaan.

Een aangepaste installatie wordt alleen aanbevolen voor ervaren gebruikers die een goede reden hebben om **AVG Anti-Virus 2012** te installeren met afwijkende instellingen, bijvoorbeeld om te voldoen aan specifieke systeemvereisten. Als u deze optie hebt geselecteerd, klikt u op de knop ***Volgende*** om naar het dialoogvenster Aangepaste opties te gaan.

Installatie van AVG-gadget

In het rechterdeelvenster staat het selectievakje voor de AVG-gadget (*ondersteund onder Windows Vista/Windows 7*). Als u de gadget wilt installeren, schakelt u het selectievakje in. De AVG-gadget is dan toegankelijk vanaf de Windows Sidebar, en biedt u directe toegang tot de belangrijkste functies van uw **AVG Anti-Virus 2012**, i.e. scannen en updates.

Knoppen

Er zijn drie knoppen beschikbaar, zoals dat ook het geval is binnen de meeste installatiedialoogvensters:

- ***Terug*** – Klik op deze knop als u terug wilt keren naar het vorige installatiedialoogvenster.
- ***Volgende*** – Klik op deze knop als u de installatie wilt voortzetten en als u wilt doorgaan met de volgende stap.
- ***Annuleren*** – Klik op deze knop als u het installatieproces onmiddellijk wilt afsluiten. **AVG Anti-Virus 2012** wordt niet geïnstalleerd.

3.4. Aangepaste opties

In het dialoogvenster ***Aangepaste opties*** kunt u twee parameters opgeven voor de installatie:

Doelmap

In het gedeelte ***Doelmap*** geeft u op waar u **AVG Anti-Virus 2012** wilt installeren. **AVG Anti-Virus 2012** wordt standaard geïnstalleerd in de map Program Files op station C:. 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.

Onderdelen selecteren

In het dialoogvenster ***Onderdelen selecteren*** staat een overzicht van alle onderdelen van **AVG Anti-Virus 2012** die kunnen worden geïnstalleerd. Als de standaardinstellingen niet voldoen, kunt u onderdelen toevoegen of verwijderen.

U kunt echter alleen kiezen uit onderdelen die deel uitmaken van de door u gekochte AVG Edition!

Als u in de lijst ***Onderdelen selecteren*** een item selecteert, wordt rechts een korte beschrijving van het onderdeel weergegeven. Raadpleeg het Onderdelenoverzicht van deze documentatie voor meer informatie over de functionaliteit van de onderdelen. Klik op de knop ***Standaard*** om de standaardconfiguratie, ingesteld door de leverancier, te herstellen.

Knoppen

Er zijn drie knoppen beschikbaar, zoals dat ook het geval is binnen de meeste installatiedialoogvensters:

- ***Terug*** – Klik op deze knop als u terug wilt keren naar het vorige installatiedialoogvenster.
- ***Volgende*** – Klik op deze knop als u de installatie wilt voortzetten en als u wilt doorgaan met de volgende stap.
- ***Annuleren*** – Klik op deze knop als u het installatieproces onmiddellijk wilt afsluiten. **AVG Anti-Virus 2012** wordt niet geïnstalleerd.

AVG Anti-Virus 2012 © 2011 Copyright AVG Technologies CZ, s.r.o. Alle rechten voorbehouden.

3.5. De AVG Werkbalk Beveiliging installeren

In het dialoogvenster ***De AVG Werkbalk Beveiliging installeren*** bepaalt u of u de AVG Werkbalk Beveiliging wilt installeren. 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 3.0 of hoger) als u de standaardinstellingen ongewijzigd laat. Dit onderdeel biedt uitgebreide online bescherming terwijl u op internet surft.*

U kunt bovendien besluiten om *AVG Secure Search (powered by Google)* in te stellen als standaardzoekmachine. Schakel in dat geval het desbetreffende selectievakje niet uit.

3.6. Installatievoortgang

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

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

Knoppen

Er is in dit dialoogvenster slechts een knop beschikbaar, de knop ***Annuleren***. Deze knop dient alleen te worden gebruikt als u het installatieproces dat wordt uitgevoerd, wilt stoppen. **AVG Anti-Virus 2012** wordt in een dergelijk geval niet geïnstalleerd.

3.7. Installatie voltooid

Het dialoogvenster ***Installatie voltooid*** vormt de bevestiging van het feit dat **AVG Anti-Virus 2012** is geïnstalleerd en geconfigureerd:

Programma voor productverbetering

In dit dialoogvenster kunt u instellen of u wilt deelnemen aan het Programma voor productverbetering (*zie het hoofdstuk Geavanceerde instellingen AVG / Programma voor productverbetering* voor gedetailleerde informatie) waarbij er anonieme informatie wordt verzameld over gedetecteerde bedreigingen met als doel om het algehele internetbeveiligingsniveau te verhogen. Laat, als u zich daar in kunt vinden, het selectievakje ***Ik ga akkoord met deelname aan het AVG 2012-programma voor internetveiligheid en het productverbeteringsprogramma ...*** ingeschakeld *(deze optie is standaard ingeschakeld)*.

Installatie bij een zakelijke licentie

Als u gebruikmaakt van een zakelijke AVG-licentie en in gevallen waarin u eerder hebt geselecteerd dat het item Extern beheer moet worden geïnstalleerd *(zie Aangepaste opties)*, is de installatie geslaagd als er een dialoogvenster met de volgende interface wordt weergegeven:

U dient AVG-Datacentergegevens op te geven – voer de verbindingsstring naar het AVG-Datacenter als volgt in: server:poort. Als die informatie op dat moment niet beschikbaar is, kunt u het veld leeg laten en kunt u de instelling later opgeven in het dialoogvenster Geavanceerde instellingen / Extern beheer. Zie de gebruikershandleiding voor de AVG Business Edition voor gedetailleerde informatie over AVG Extern beheer. U kunt deze handleiding downloaden vanaf de AVG-websitehttp://www.avg.com/).

zie het hoofdstuk Onderdelenoverzicht in dit document. Klik op de knop ***Standaard*** om de standaardconfiguratie, ingesteld door de leverancier, te herstellen.

Knoppen

In dit dialoogvenster zijn de volgende knoppen beschikbaar

- ***Voltooien*** – Klik hierop om het installatieproces te voltooien, zodat u kunt profiteren van de beveiliging die wordt geboden door **AVG Anti-Virus 2012**.

4. Na de installatie

4.1. Productregistratie

Neem nadat u de installatie van **AVG Anti-Virus 2012** hebt voltooid even de tijd om uw product online te registreren op de AVG-website (http://www.avg.com/). Na de registratie beschikt u over volledige toegang tot uw AVG-gebruikersaccount, de nieuwsbrief van AVG Update en andere services die alleen beschikbaar zijn voor geregistreerde gebruikers.

De eenvoudigste manier waarop u het programma kunt registreren, is door dit rechtstreeks vanuit de gebruikersinterface van **AVG Anti-Virus 2012** te doen. Selecteer in het hoofdmenu Help/Nu registreren. De ***registratie*** pagina op de AVG-website (http://www.avg.com/) wordt geopend. Volg de instructies die op deze pagina worden weergegeven.

4.2. Toegang tot gebruikersinterface

Het AVG-hoofddialoogvenster kan op verscheidene manieren worden geopend:

- dubbelklik op het AVG-pictogram in het systeemvak
- dubbelklik op het pictogram van AVG op het bureaublad
- dubbelklik op de statusregel onder in de AVG gadget (*als die is geïnstalleerd; ondersteund door Windows Vista/ Windows 7*)
- kies ***Start/Programma's/AVG 2012/AVG Gebruikersinterface***

4.3. Volledige computerscan

Het risico bestaat dat er een computervirus naar uw computer is overgebracht voordat u **AVG Anti-Virus 2012** 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.

4.4. De EICAR-test

Als u zeker wilt weten of **AVG Anti-Virus 2012** 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. Onmiddellijk nadat u het

downloaden van het testbestand hebt bevestigd, wordt er door de component Online Shield (*van het onderdeel Link Scanner*) een waarschuwing weergegeven. 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 staat toe dat het bestand wordt gedownload en opgeslagen op de lokale schijf, maar zodra u probeert om het bestand uit te pakken, wordt er door Resident Shield (*binnen het onderdeel Anti-Virus*) een 'virus' gedetecteerd.

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

4.5. AVG-standaardconfiguratie

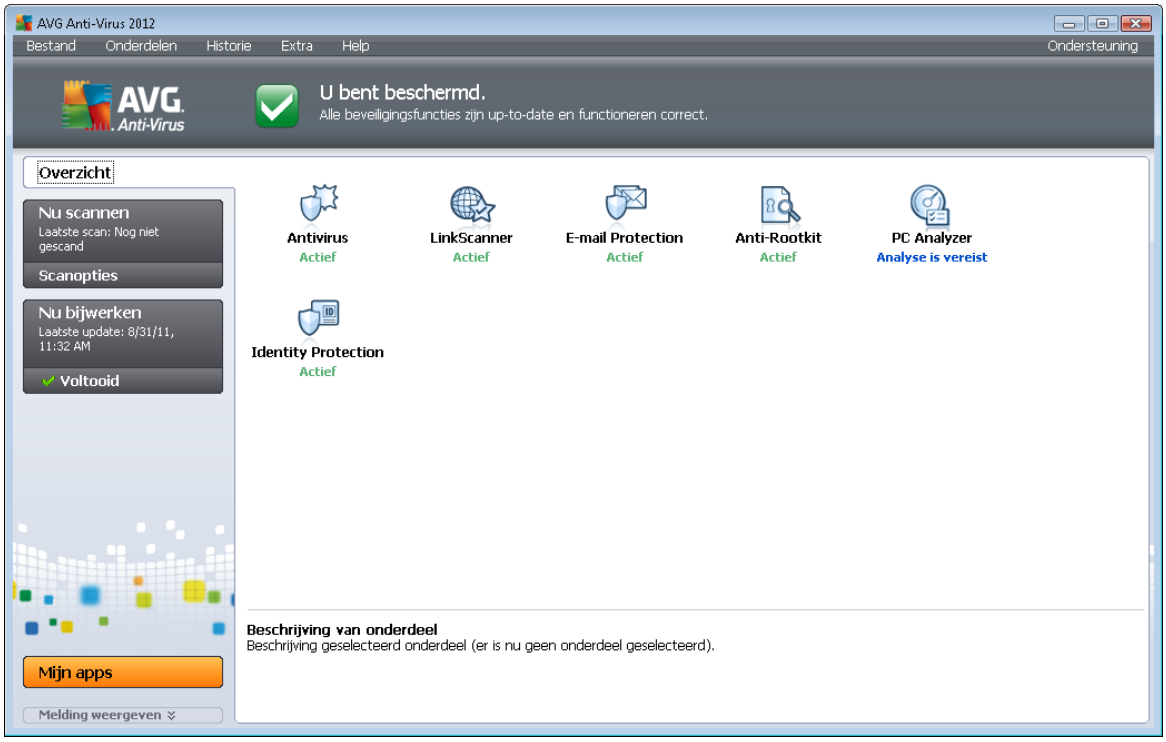
De standaardconfiguratie (*dat wil zeggen de manier waarop de toepassing functioneert meteen na installatie*) van **AVG Anti-Virus 2012** is het werk van de leverancier van de software: alle onderdelen en functies zijn zo ingesteld dat de toepassing optimaal presteert.

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 het venster met Geavanceerde instellingen AVG: open het menu ***Extra -> Geavanceerde instellingen*** en bewerk de configuratie van AVG in het dialoogvenster Geavanceerde instellingen AVG dat dan wordt geopend.

5. AVG-gebruikersinterface

AVG Anti-Virus 2012 wordt geopend met het hoofdvenster:



Het hoofdvenster is onderverdeeld in een aantal secties:

- ***Het systeemmenu*** *(de menubalk boven in het venster)* is het standaardmenu voor het openen van alle onderdelen, services en functies van **AVG Anti-Virus 2012** - details >>
- ***In de sectie Info Beveiligingsstatus*** *(bovenste deel van het venster)* vindt u informatie over de huidige status van **AVG Anti-Virus 2012** - details >>
- ***De snelkoppelingen*** *(linkerdeel van het venster)* bieden u snelle toegang tot de belangrijkste en meest gebruikte taken van **AVG Anti-Virus 2012** - details >>
- Δεκνοπ***Mijn apps*** *(linksonder in het venster)* biedt toegang tot een overzicht van aanvullende toepassingen die beschikbaar zijn voor **AVG Anti-Virus 2012**: LiveKive, Family Safety en PC Tuneup
- ***Het onderdelenoverzicht*** *(centrale sectie van het venster)* geeft een overzicht van alle geïnstalleerde onderdelen van **AVG Anti-Virus 2012 -** details >>
- ***Het pictogram in het systeemvak*** *(rechtsonder in het scherm, in het systeemvak)* geeft de huidige status aan van **AVG Anti-Virus 2012** - details >>
- ***De AVG gadget*** *(in Windows Sidebar, ondersteund in Windows Vista/7)* biedt snelle toegang tot scans en updates van **AVG Anti-Virus 2012** - details>>

5.1. Systeemmenu

De ***menubalk*** is de standaardingang voor de navigatiestructuur die in alle Windows-toepassingen wordt gebruikt. Deze is horizontaal aan de bovenrand van het hoofdvenster van **AVG Anti-Virus 2012** geplaatst. Met behulp van het systeemmenu heeft u toegang tot de AVG onderdelen, functies en services.

Het systeemmenu is onderverdeeld in vijf secties:

5.1.1. Bestand

- ***Afsluiten*** - afsluiten van de **AVG Anti-Virus 2012**-gebruikersinterface. De AVG toepassing zal echter op de achtergrond actief blijven en uw computer is nog steeds beschermd!

5.1.2. Onderdelen

Het menu Onderdelen heeft koppelingen voor het openen van de standaardpagina van alle geïnstalleerde AVG-onderdelen:

- ***Systeemoverzicht*** – weergeven van het standaard dialoogvenster met het overzicht van alle geïnstalleerde onderdelen en hun status
- ***Anti-Virus*** detecteert virussen, spyware, wormen, Trojaanse paarden, ongewenste uitvoerbare bestanden en bibliotheken op uw systeem en beschermt u tegen schadelijke adware - details >>
- ***LinkScanner*** beschermt u tegen aanvallen vanaf internet als u zoekt of surft op internet - details >>
- ***E-mail Protection*** controleert uw binnenkomende e-mailberichten op spam en blokkeert virussen, phishingaanvallen en andere bedreigingen - details >>
- ***Anti-Rootkit*** scant toepassingen, stuurprogramma's en DLL-bibliotheken op zoek naar gevaarlijke rootkits. - details >>
- ***PC Analyzer*** Verzorgt informatie over de status van de computer – details >>
- ***Identity Protection*** beschermt uw digitale bezittingen voortdurend tegen nieuwe en onbekende bedreigingen - details >>
- ***Werkbalk Beveiliging*** biedt AVG-functionaliteit die direct beschikbaar is vanuit de webbrowser – details >>
- ***Remote Administration*** wordt alleen weergegeven in AVG Business Editions als u tijdens het installatieproces hebt aangegeven dat het onderdeel moest worden geïnstalleerd

5.1.3. Historie

- Scanresultaten - De AVG testinterface wordt geopend. Dit is het 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 de Online Shield-service van het onderdeel LinkScanner

- Quarantaine - De interface van de Quarantaine wordt geopend, waarin 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

- Logboek Eventhistorie – het dialoogvenster wordt geopend met de geschiedenis van alle vastgelegde **AVG Anti-Virus 2012acties van**

5.1.4. Extra

- 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 afzonderlijk bestand selecteren dat u wilt scannen.

- Update – hiermee kunt u automatisch de updateprocedure van **AVG Anti-Virus 2012** starten.

- ***Bijwerken vanuit directory...*** – de updateprocedure wordt gestart aan de hand van updatebestanden in een opgegeven map op de lokale vaste schijf. Deze optie wordt echter alleen aanbevolen als noodprocedure, bijvoorbeeld onder omstandigheden waarbij er geen verbinding is met internet (*uw computer is bijvoorbeeld geïnfecteerd en afgesloten van internet; uw computer is aangesloten op een netwerk zonder verbinding met internet, enz.*). Selecteer in het venster dat wordt geopend, de map waarin u eerder het updatebestand hebt opgeslagen, en start de updateprocedure.

- Geavanceerde instellingen... – het dialoogvenster AVG Geavanceerde instellingen wordt geopend waarin u de configuratie van AVG Anti-Virus 2012 kunt wijzigen. Over het algemeen is het raadzaam de standaardinstellingen aan te houden, zoals deze zijn ingesteld door de leverancier van de software.

5.1.5. 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 wordt geopend (http://www.avg.com/)
- ***Over virussen en bedreigingen*** – De online Virusencyclopedie wordt geopend, waarin u kunt zoeken naar gedetailleerde informatie over een herkend virus
- ***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*** - Er wordt verbinding gemaakt met de registratiepagina van de AVG-website (http://www.avg.com/). Voer uw registratiegegevens in. Uitsluitend klanten die hun AVG-product registreren, komen in aanmerking voor gratis technische ondersteuning.

Opmerking*: als u de evaluatieversie van* **AVG Anti-Virus 2012** *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 Anti-Virus 2012** *hebt geïnstalleerd met een verkoopnummer, worden deze items weergegeven als* ***Registreren*** *en* ***Activeren****.*

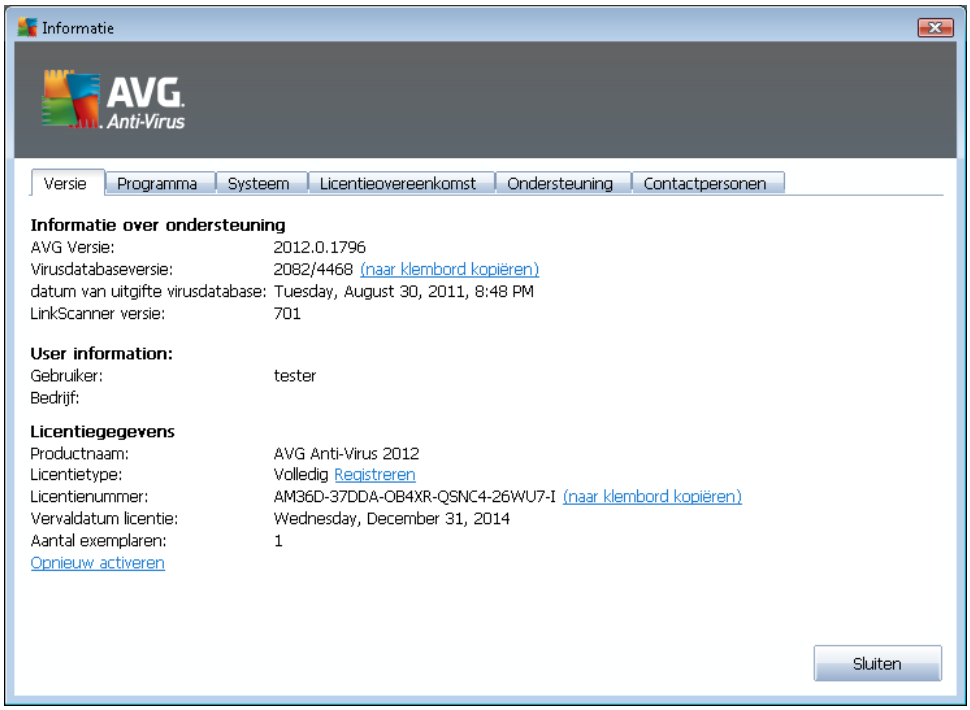
- ***Info over AVG*** - Het dialoogvenster ***Info*** wordt geopend met vijf tabbladen met gegevens over de programmanaam, versie van programma en virusdatabase, systeeminformatie, licentieverklaring en contactgegevens van ***AVG Technologies CZ***.

5.1.6. Ondersteuning

Als u op de koppeling ***Ondersteuning*** klikt, wordt het dialoogvenster ***Informatie*** geopend. Dit dialoogvenster bevat informatie die u mogelijk nodig hebt wanneer u behoefte hebt aan hulp. Het dialoogvenster omvat basisgegevens over het geïnstalleerde AVG-programma (*programma-/databaseversie*), gedetailleerde licentie-informatie en een lijst met snelkoppelingen voor ondersteuning:

Het dialoogvenster ***Informatie*** kent zes tabbladen:

het tabblad ***Versie*** is verdeeld in drie secties:

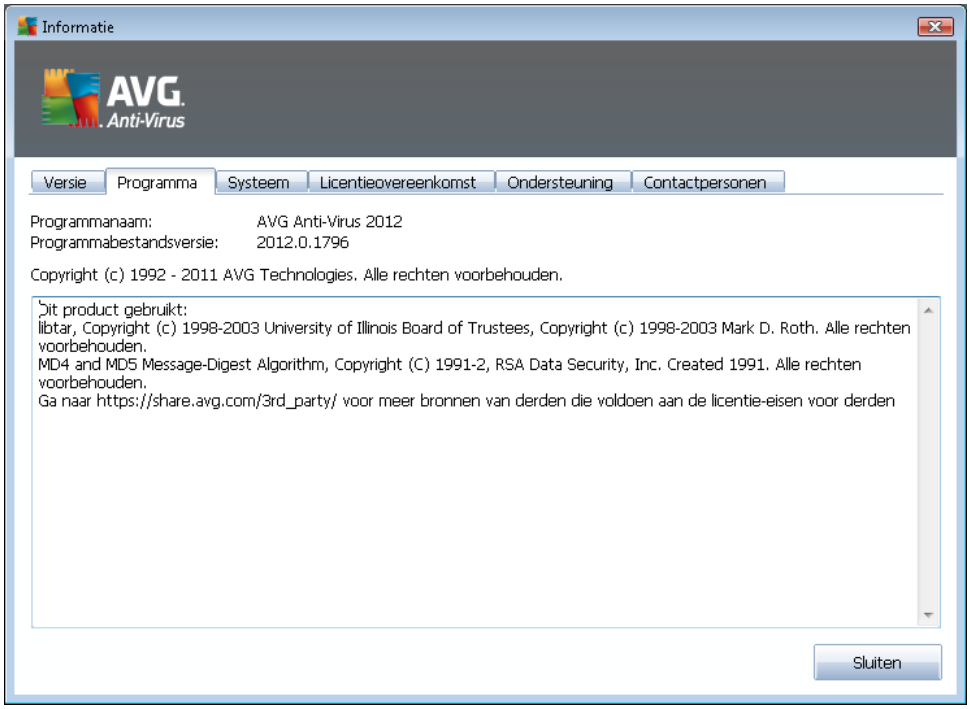


- ***Informatie over ondersteuning*** - Deze sectie biedt informatie over de **AVG Anti-Virus 2012** versie, de virusdatabaseversie, de Antispam-databaseversie en de LinkScanner-versie.

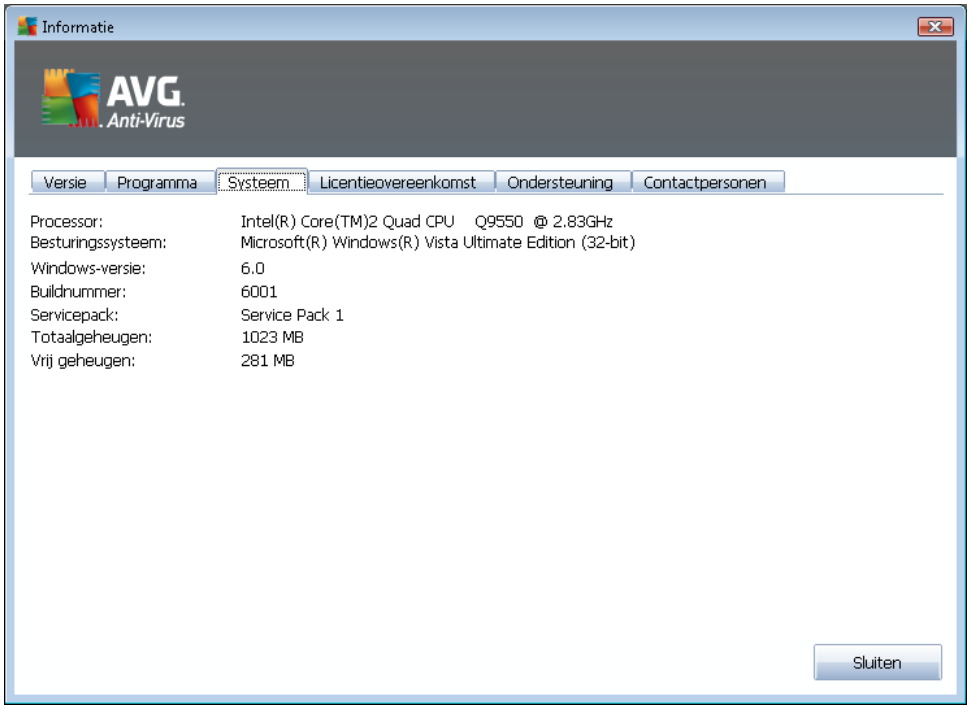
- ***Gebruikersinformatie*** - Deze sectie biedt informatie over de gebruiker en het bedrijf waartoe de licentie behoort.

- ***Licentiegegevens*** - Deze sectie biedt informatie over uw licentie *(productnaam, licentietype, licentienummer, vervaldatum en aantal exemplaren*). Deze sectie bevat tevens de koppeling ***Registreren*** die u kunt gebruiken om **AVG Anti-Virus 2012** online te registreren. Op deze wijze kunt u de technische ondersteuning van AVG ten volle benutten. Daarnaast kunt u de koppeling ***Opnieuw activeren*** gebruiken om het dialoogvenster ***AVG activeren*** te openen: vul uw licentienummer in in het desbetreffende veld als u uw verkoopnummer wilt vervangen *(het nummer dat u tijdens de installatie van AVG Anti-Virus 2012 hebt ingevoerd)* of om uw huidige licentienummer te vervangen door een ander nummer *(zoals wanneer u een upgrade naar een hoger AVG-product uitvoert).*

Op het tabblad ***Programma*** wordt informatie weergegeven over de versie van het **AVG Anti-Virus 2012**-programmabestand en over code van derden die in het product wordt gebruikt:

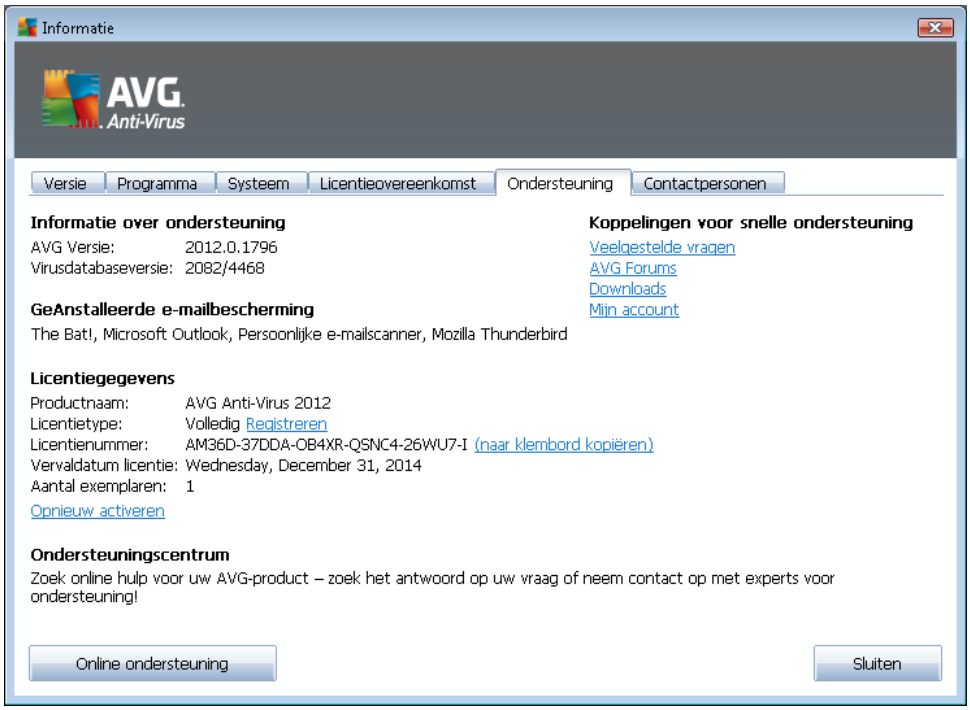


Het tabblad ***Systeem*** biedt een lijst met parameters van uw besturingssysteem *(processortype, besturingssysteem en de versie daarvan, buildnummer, toegepaste servicepacks, totale geheugengrootte en hoeveelheid vrij geheugen)*:

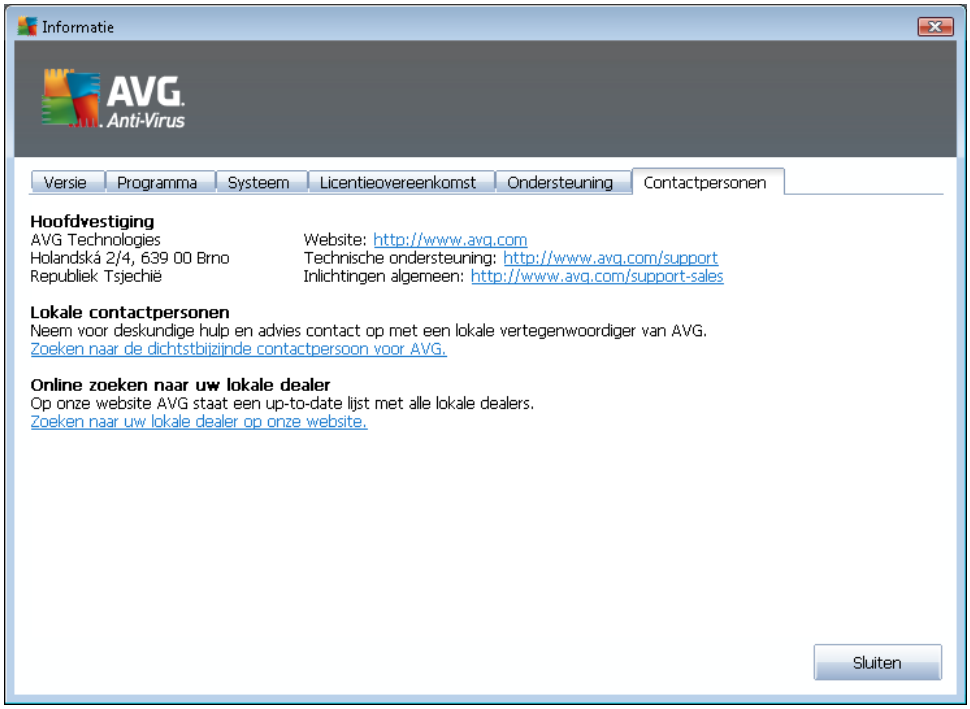


Op het tabblad ***Licentieovereenkomst*** wordt de volledige tekst van de licentieovereenkomst tussen u en AVG Technologies weergegeven:

Op het tabblad ***Ondersteuning*** wordt een lijst weergegeven met alle contactmogelijkheden die u kunt gebruiken als u contact wilt opnemen met de klantenondersteuningsservice. Daarnaast worden er koppelingen weergegeven voor de AVG-website (http://www.avg.com/), AVG-forums, FAQ, enzovoort. Tot slot wordt er ook informatie weergegeven die u mogelijk nodig hebt wanneer u contact opneemt met het ondersteuningsteam:



Het tabblad ***Contactpersonen*** bevat een lijst met alle contactgegevens voor AVG Technologies en voor plaatselijke AVG-vertegenwoordigers en wederverkopers:



5.2. Info Beveiligingsstatus

De sectie ***Info Beveiligingsstatus*** bevindt zich in het bovenste gedeelte van het hoofdvenster van **AVG Anti-Virus 2012**. In deze sectie staat altijd informatie over de huidige beveiligingsstatus van **AVG Anti-Virus 2012**. Hieronder volgt een overzicht van de pictogrammen die in deze sectie kunnen worden weergegeven, en hun betekenis:

- Het groene pictogram geeft aan dat ***AVG Anti-Virus 2012 volledig naar behoren werkt***. Uw computer is volledig beveiligd, de bestanden zijn bijgewerkt en alle geïnstalleerde onderdelen werken correct.

- Een 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 Anti-Virus 2012**. U hebt een onderdeel mogelijk om de een of andere reden uitgeschakeld. De beveiliging is nog steeds ingeschakeld. 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***.

Het oranje pictogram wordt ook weergegeven als u om een of andere reden hebt besloten om

de foutstatus van een onderdeel te negeren. De optie ***Onderdeelstatus negeren*** wordt weergegeven in het snelmenu (*dat wordt geopend wanneer u met de rechtermuisknop op*) het desbetreffende onderdeel klikt in het onderdelenoverzicht in het hoofdvenster van **AVG Anti-Virus 2012**. Selecteer deze optie als u wilt aangeven dat u zich bewust bent van de foutstatus van een onderdeel en dat u om welke reden ook **AVG Anti-Virus 2012** zo wilt instellen dat u niet wordt gewaarschuwd via het systeemvakpictogram. Het kan zijn dat u deze optie in een specifieke situatie moet gebruiken. U wordt in een dergelijk geval echter aangeraden om de optie ***Onderdeelstatus negeren*** zo snel mogelijk uit te schakelen.

- Het rode pictogram geeft aan dat ***AVG Anti-Virus 2012 in een kritieke situatie verkeert***. Eén of meer onderdelen functioneren niet goed en **AVG Anti-Virus 2012** 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.

In gevallen waarin AVG Anti-Virus 2012 niet is ingesteld voor optimale prestaties, wordt er naast de informatie over de beveiligingstatus een nieuw knop met de naam Repareren (of Alles repareren als het probleem meerdere onderdelen betreft) weergegeven. Klik op die knop om een automatisch proces voor programmacontrole en -configuratie te starten. U kunt op deze wijze AVG Anti-Virus 2012 instellen met het oog op maximale prestaties en een maximaal beveiligingsniveau.

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 de statusinformatie van AVG Anti-Virus 2012 ook opvragen via het systeemvakpictogram.*

5.3. Snelkoppelingen

Snelkoppelingen bevinden zich links in de **AVG Anti-Virus 2012**-gebruikersinterface. Deze koppelingen bieden onmiddellijke toegang tot de belangrijkste en meest gebruikt functies van de toepassing, zoals scannen en bijwerken De snelkoppelingen zijn toegankelijk vanuit alle dialoogvensters in de gebruikersinterface:

Snelkoppelingen zijn op een grafische wijze onderverdeeld in drie secties:

- ***Overzicht*** - Gebruik deze koppeling als u van het huidige geopende AVG-dialoogvenster wilt

schakelen naar het standaardvenster met een overzicht van alle geïnstalleerde onderdelen. *(Zie het hoofdstuk Overzicht van onderdelen voor gedetailleerde informatie)*

- ***Nu scannen*** - De knop biedt standaard toegang tot informatie over de als laatste gestarte scan *(waaronder het scantype en de datum waarop deze scan is gestart)*. Klik op de opdracht ***Nu scannen*** als u dezelfde scan opnieuw wilt starten. Klik op de koppeling ***Scanopties*** als u een andere scan wilt starten. U opent op deze wijze de AVG-scaninterface waarin u scans kunt uitvoeren en waarin u de parameters van scans kunt bewerken. *(Zie het hoofdstuk AVG-scans voor gedetailleerde informatie)*

- ***Nu bijwerken*** - Deze koppeling biedt toegang tot informatie over de datum en het tijdstip waarop het bijwerken voor het laatst is gestart. Druk op de knop als u het bijwerken onmiddellijk wilt uitvoeren en als u de voortgang van het bijwerken wilt volgen. *(Zie het hoofdstuk AVG-updates voor gedetailleerde informatie)*

Snelkoppelingen zijn op elk gewenst moment toegankelijk vanuit de AVG-gebruikersinterface. Als u een snelkoppeling gebruikt om een specifiek proces uit te voeren (een scan of een update), schakelt de toepassing naar een nieuw dialoogvenster, waarbij de snelkoppelingen beschikbaar blijven. Daarnaast wordt het proces dat wordt uitgevoerd grafisch weergegeven in het navigatiegedeelte, zodat u over de volledige controle beschikt met betrekking tot alle gestarte processen die op dat moment binnen **AVG Anti-Virus 2012** worden uitgevoerd.

5.4. Overzicht van onderdelen

Sectie met het onderdelen overzicht

De sectie met het ***onderdelenoverzicht*** bevindt zich in het middengedeelte van de **AVG Anti-Virus 2012**-gebruikersinterface. De sectie is onderverdeeld in twee gedeelten:

- ***Een overzicht met alle geïnstalleerde onderdelen***, dat grafische deelvensters voor alle geïnstalleerde onderdelen omvat. Elk deelvenster wordt aangegeven met een pictogram voor het onderdeel en biedt informatie met betrekking tot het momenteel wel of niet actief zijn van het desbetreffende onderdeel.

- ***De onderdeelbeschrijving*** wordt weergegeven in het onderste gedeelte van dit dialoogvenster. In de beschrijving wordt de basisfunctionaliteit van het onderdeel beknopt toegelicht. Daarnaast wordt er informatie weergegeven over de huidige status van het geselecteerde onderdeel.

Lijst met geïnstalleerde onderdelen

De sectie ***Overzicht van onderdelen*** in **AVG Anti-Virus 2012** bevat informatie over de volgende onderdelen:

- ***Anti-Virus*** detecteert virussen, spyware, wormen, Trojaanse paarden, ongewenste uitvoerbare bestanden en bibliotheken op uw systeem en beveiligt u tegen schadelijke adware - details >>

- ***LinkScanner*** beveiligt u tegen aanvallen vanaf internet als u zoekt of surft op internet - details >>
- ***E-mail Protection*** controleert uw binnenkomende e-mailberichten op spam en blokkeert virussen, phishingaanvallen en andere bedreigingen - details >>
- ***Anti-Rootkit*** scant toepassingen, stuurprogramma's en DLL-bibliotheken op zoek naar gevaarlijke rootkits - details >>
- ***PC Analyzer*** Verzorgt informatie over de status van de computer – details >>
- ***Identity Protection*** beveiligt uw digitale bezittingen voortdurend tegen nieuwe en onbekende bedreigingen - details >>
- ***Werkbalk Beveiliging*** AVG-functionaliteit direct beschikbaar vanuit de webbrowser – details >>

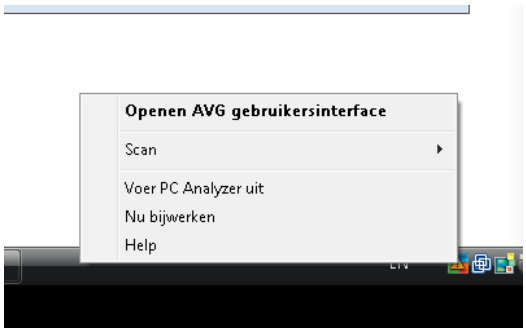
- ***Extern beheer*** wordt alleen weergegeven in AVG Business Editions als u tijdens het installatieproces hebt aangegeven dat het onderdeel moest worden geïnstalleerd

Beschikbare acties

- ***Beweeg de muis over een onderdeelpictogram*** om dit binnen het onderdelenoverzicht te markeren. Hierbij wordt in het onderste gedeelte van de gebruikersinterface een beschrijving weergegeven van de basisfunctionaliteit van het onderdeel.
- ***Als u één keer klikt op het pictogram van een onderdeel***, wordt de eigen interface van het onderdeel geopend met een lijst met statistische basisgegevens.
- ***Als u met de rechtermuisknop op het pictogram van een onderdeel*** klikt, wordt er een snelmenu met verscheidene opties weergegeven:
  - ***Openen*** – Klik op deze optie om het eigen dialoogvenster van het onderdeel te openen *(dit is ook mogelijk door één keer op het pictogram van het onderdeel te klikken)*.
  - ***Onderdeelstatus negeren*** - Selecteer deze optie om aan te geven dat u zich bewust bent van de foutstatus van het onderdeel en dat u om welke reden dan ook deze status wilt handhaven, zonder dat u via het systeemvakpictogram wordt gewaarschuwd.
  - ***Openen in geavanceerde instellingen...*** - Deze optie is uitsluitend beschikbaar voor onderdelen die de mogelijkheid bieden tot het instellen van geavanceerde instellingen.

5.5. Systeemvakpictogram

Het AVG-systeemvakpictogram *(op de Windows-taakbalk, rechts onder in de hoek van uw scherm)* geeft de status van **AVG Anti-Virus 2012** aan. Het pictogram is altijd zichtbaar in het systeemvak, ongeacht of de gebruikersinterface van **AVG Anti-Virus 2012** is geopend of gesloten:



Weergave van het AVG-systeemvakpictogram

- Als alle kleuren worden weergegeven, zonder dat er elementen aan het pictogram zijn toegevoegd, geeft het pictogram aan dat alle **AVG Anti-Virus 2012**onderdelen actief en naar behoren werken. Dit pictogram wordt echter op dezelfde wijze weergegeven als een van de onderdelen niet naar behoren werkt en de gebruiker heeft besloten om de onderdeelstatus te negeren. *(Als u hebt bevestigd dat de onderdeelstatus moet worden genegeerd, geeft u daarmee aan dat zich bewust bent van de foutstatus van het onderdeel, maar dat u om de een of andere reden niet met betrekking tot deze situatie wenst te worden gewaarschuwd.)*

- Het pictogram met een uitroepteken geeft aan dat er op een onderdeel *(of meerdere onderdelen)* een foutstatus van toepassing is. Besteed altijd aandacht aan een dergelijke waarschuwing en probeer het configuratieprobeem weg te nemen als een onderdeel niet naar behoren is ingesteld. Als u wijzigingen in de configuratie van een onderdeel wilt aanbrengen, dubbelklikt u op het systeemvakpictogram om de gebruikersinterface van de toepassing te openen. Raadpleeg de sectie over beveiligingsstatusinformatie voor gedetailleerde informatie over op welk onderdeel een foutstatus van toepassing is.

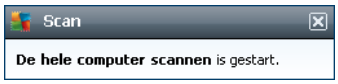
- Het is tevens mogelijk dat het systeemvakpictogram in alle kleuren wordt weergegeven met een knipperende, roterende lichtstraal. Deze grafische weergave geeft aan dat er momenteel een update wordt uitgevoerd.

- De alternatieve weergave van het pictogram in alle kleuren met een pijl geeft aan dat er **AVG Anti-Virus 2012** scans worden uitgevoerd.

Informatie bij het AVG-systeemvakpictogram

Het AVG-systeemvakpictogram biedt daarnaast informatie over huidige activiteiten binnen **AVG Anti-Virus 2012** en over mogelijke statuswijzigingen in het programma (*zoals het automatisch starten van een scan of update, een wijziging van een onderdeelstatus, een foutstatus, ...*) via een

pop-upvenster dat wordt geopend vanuit het systeemvakpictogram van:



Acties die toegankelijk zijn via het AVG-systeemvakpictogram

Het AVG-systeemvakpictogram kan tevens worden gebruikt als een koppeling voor het openen van de gebruikersinterface van **AVG Anti-Virus 2012**. Dubbelklik daartoe op het pictogram. Als u met de rechtermuisknop op het pictogram klikt, wordt er een beknopt snelmenu weergegeven, dat de volgende opties bevat:

- ***Openen AVG-gebruikersinterface*** – Hiermee opent u de gebruikersinterface van **AVG Anti-Virus 2012**.
- ***Scan*** – Klik hierop om het snelmenu met vooraf gedefinieerde scans (*De hele computer scannen*, *Mappen of bestanden scannen*, *Anti-Rootkitsscan*) te openen en selecteer de gewenste scan. De scan wordt onmiddellijk gestart. .
- ***PC Analyzer*** uitvoeren - Hiermee kunt u het onderdeel PC Analyzer starten.
- ***Scans die worden uitgevoerd*** - Dit item wordt uitsluitend weergegeven wanneer er een scan op uw computer wordt uitgevoerd. U kunt vervolgens de scanprioriteit voor die scan wijzigen, de scan onderbreken of afbreken. Bovendien zijn de volgende acties mogelijk: *Prioriteit instellen voor alle scans*, *Alle scans onderbreken* en *Alle scans afbreken*.
- ***Nu bijwerken*** - Hiermee start u een onmiddellijke update.
- ***Help*** - Hiermee opent u het Help-bestand op de startpagina.

5.6. AVG-gadget

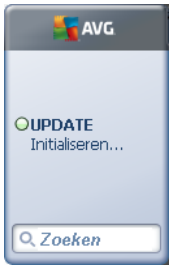
AVG gadget wordt weergegeven op het Windows Bureaublad(*Windows Sidebar*). De toepassing wordt alleen ondersteund voor de besturingssystemen Windows Vista en Windows 7. ***AVG gadget*** biedt directe toegang tot de belangrijkste functies van **AVG Anti-Virus 2012**, namelijk scannen en updates:

Snelle toegang tot scannen en bijwerken

Indien nodig, stelt ***AVG gadget*** u in staat om onmiddellijk een scan of update te starten:

- ***Nu scannen*** – als u op de koppeling ***Nu scannen*** klikt, wordt de scan De hele computer scannen gestart. U kunt de voortgang van de scan volgen in de gebruikersinterface van de gadget. Een beknopt overzicht met cijfers biedt informatie over het aantal gescande objecten, gedetecteerde bedreigingen en verholpen bedreigingen. U kunt het scannen op elk gewenst moment onderbreken of afbreken. Zie het standaarddialoogvenster Overzicht scanresultaten voor meer informatie over de scanresultaten. U opent dit dialoogvenster rechtstreeks vanuit de gadget met de optie ***Details weergeven*** *(de desbetreffende scanresultaten staan bij Sidebar-gadgetscan)*.

- ***Nu bijwerken*** – als u op de koppeling ***Nu bijwerken*****AVG Anti-Virus 2012** klikt, wordt de update direct vanuit de gadget gestart:



Toegang tot sociale netwerken

AVG gadget biedt u tevens snelkoppeling naar de belangrijkste sociale netwerken. Gebruik de desbetreffende knop als u verbinding wilt maken met AVG-community's in Twitter, Facebook, of LinkedIn:

- ***Twitter-koppeling*** – Hiermee wordt een nieuwe ***AVG gadget***-interface geopend met een overzicht van de nieuwste AVG-feeds op Twitter. Klik op de koppeling ***Alle AVG Twitter feeds weergeven*** om een nieuw venster te openen in uw internetbrowser met de website van Twitter, in het bijzonder de pagina met nieuws over en van AVG:

- ***Facebook-koppeling*** – de website van Facebook openen in de internetbrowser, in het bijzonder de pagina van de ***AVG community***

- ***LinkedIn*** – Deze optie is alleen beschikbaar bij de netwerkinstallatie (*dat wil zeggen dat u AVG hebt geïnstalleerd met een AVG Business Edition-licentie*). De internetbrowser wordt geopend met daarin de website ***AVG SMB Community*** in het sociale netwerk LinkedIn

Andere functies die toegankelijk zijn via de gadget

- ***PC Analyzer*** – Hiermee kunt u de gebruikersinterface van PC Analyzer openen

- ***Zoekvak*** – na het invoeren van een zoekterm worden de resultaten meteen weergegeven in een venster dat wordt geopend in de standaardwebbrowser

6. AVG-onderdelen

6.1. Antivirus

Het onderdeel ***Anti-Virus*** is een hoeksteen van **AVG Anti-Virus 2012** en combineert verscheidene fundamentele functies van een beveiligingsprogramma:

- Scanengine
- Residente beveiliging
- Beveiliging tegen spyware

6.1.1. Scanprogramma

Het scanprogramma vormt de basis van het onderdeel ***Anti-Virus*** en scant alle bestanden en bestandsactiviteiten *(openen/sluiten van bestanden, enzovoort)* op bekende virussen. Elk gedetecteerd virus wordt geblokkeerd, zodat dit geen acties kan uitvoeren. Het virus wordt daarna onschadelijk gemaakt of in quarantaine geplaatst.

De belangrijkste functie van de AVG Anti-Virus 2012-beveiliging is ervoor zorgen dat er geen enkel bekend virus op de computer kan worden uitgevoerd.

Detectiemethoden

De meeste antivirusprogramma's maken ook gebruik van heuristische analyse, waarbij bestanden worden gescand op standaardkenmerken van virussen, zogeheten virale handtekeningen. Dat betekent dat de virusscanner een nieuw, nog onbekend virus kan detecteren, als dat virus bepaalde typerende kenmerken heeft van bestaande virussen. ***Anti-Virus*** gebruikt de volgende detectiemethoden:

- Scannen – zoeken naar tekenreeksen die kenmerkend voor een bepaald virus zijn
- *Heuristische analyse* - Dynamische emulatie van de instructies van het gescande object in een virtuele computeromgeving
- *Algemene detectie* – detectie van instructies die kenmerkend zijn voor een bepaald virus of een bepaalde groep virussen

Aangezien bij het gebruik van slechts één technologie een bepaald virus mogelijk over het hoofd wordt gezien of niet wordt herkend, zijn in ***Anti-Virus*** diverse technologieën gecombineerd om te garanderen dat uw computer tegen virussen is beveiligd. **AVG Anti-Virus 2012** is tevens in staat om uitvoerbare toepassingen en DLL-bibliotheken te analyseren en te detecteren die binnen het systeem mogelijk ongewenst zijn. Dergelijke bedreigingen worden aangeduid als Potentieel ongewenste programma's *(verschillende typen spyware, adware, enzovoort).*. Daarnaast scant **AVG Anti-Virus 2012** uw systeemregister op verdachte vermeldingen, tijdelijke internetbestanden en zogeheten tracking-cookies. U kunt hierbij instellen dat alle mogelijk schadelijke items op dezelfde wijze moeten worden afgehandeld als andere infecties.

AVG Anti-Virus 2012 biedt ononderbroken beveiliging voor uw computer.

6.1.2. Residente beveiliging

AVG Anti-Virus 2012 biedt een ononderbroken beveiliging in de vorm van een zogeheten residente beveiliging. Het onderdeel ***Anti-Virus*** scans elk bestand *(met uitzondering van specifieke extensies en bestanden zonder extensies)* dat wordt geopend, opgeslagen of gekopieerd. Dit onderdeel bewaakt de systeemgebieden van de computer, verwijderbare media (*flashschijven, enzovoort*). Als er een virus wordt gedetecteerd in een bestand dat wordt geopend, wordt de bewerking die wordt uitgevoerd, onderbroken, zodat het virus niet kan worden geactiveerd. Normaal gesproken merkt u niets van dit proces aangezien de residente beveiliging op de achtergrond wordt uitgevoerd. U wordt uitsluitend gewaarschuwd wanneer er bedreigingen worden gevonden. Tegelijkertijd blokkeert ***Anti-Virus*** het activeren van bedreigingen en verwijdert dit onderdeel bedreigingen.

De residente beveiliging wordt in het geheugen van de computer geladen tijdens het opstarten. Het is cruciaal dat u deze ingeschakeld houdt.

6.1.3. Beveiliging tegen spyware

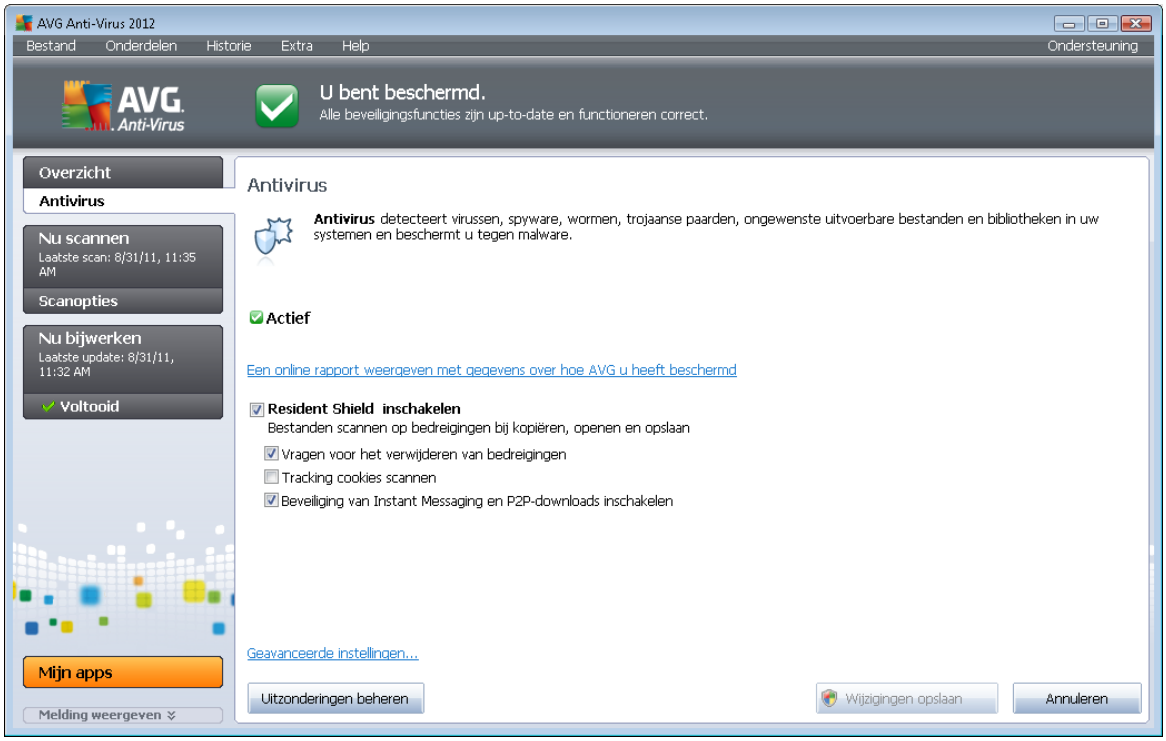
Anti-Spyware bestaat uit een spywaredatabase die wordt gebruikt voor het identificeren van bekende typen spywaredefinities. AVG-spywaredeskundigen werken hard om de meest recente spywarepatronen in kaart te brengen en te beschrijven zodra deze opduiken en vervolgens voegen ze de definities toe aan de database. Met behulp van het updateproces worden die nieuwe definities vervolgens naar uw computer gedownload, zodat u altijd kunt vertrouwen op bescherming tegen zelfs de nieuwste vormen van spyware. ***Anti-Spyware*** stelt u in staat om uw computer volledig te scannen op malware/spyware. Het onderdeel detecteert ook slapende en niet-actieve malware, dat wil zeggen malware die al wel is gedownload, maar die nog niet is geactiveerd.

Wat is spyware

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.

6.1.4. Antivirus-interface

In de interface van het onderdeel ***Anti-Virus*** worden beknopte informatie over de functionaliteit van het onderdeel, informatie over de huidige status van het onderdeel *(Actief)* en basisconfiguratieopties voor het onderdeel weergegeven:



Configuratieopties

Het dialoogvenster bevat een aantal elementaire configuratieopties voor functies die binnen het onderdeel ***Anti-Virus*** beschikbaar zijn. Hierna volgt een aantal korte beschrijvingen daarvan:

- ***Een online rapport weergeven met gegevens over hoe AVG u heeft beschermd*** – De koppeling leidt naar een specifieke pagina op de AVG-website (http://www.avg.com/). Op deze pagina vindt u een gedetailleerd overzicht van alle **AVG Anti-Virus 2012** activiteiten die op uw computer zijn uitgevoerd binnen een specifieke periode en in totaal.

- ***Resident Shield inschakelen*** – Deze optie stelt u in staat om de residente beveiliging op een eenvoudige wijze in of uit te schakelen. Resident Shield scant bestanden als deze worden gekopieerd, geopend of opgeslagen. Wanneer een virus of welke bedreiging dan ook wordt gedetecteerd, wordt u onmiddellijk gewaarschuwd. Deze functie is standaard ingeschakeld en het wordt aanbevolen om dit zo te houden. Als de residente beveiliging is ingeschakeld, kunt u bepalen op welke wijze de mogelijk gedetecteerde infecties moeten worden behandeld:

    - ***Alle bedreigingen automatisch verwijderen*** / ***Vragen voor het verwijderen van bedreigingen*** - Selecteer een van deze opties. Deze keuze heeft geen invloed op het beveiligingsniveau en brengt uitsluitend uw voorkeur tot uitdrukking.

    - ***Tracking cookies scannen*** – U kunt los van eerdere opties bepalen of u wilt scannen op tracking cookies. *(Cookies zijn tekstpakketten die door een server naar een webbrowser worden verzonden en die vervolgens telkens als de browser weer contact maakt met deze server, ongewijzigd naar de server worden teruggezonden.*

HTTP-cookies worden gebruikt voor het verifiëren, traceren en bijhouden van bepaalde informatie over gebruikers, zoals voorkeuren voor websites of de inhoud van winkelwagentjes.) In specifieke gevallen kunt u deze optie inschakelen om een maximaal beveiligingsniveau te bewerkstelligen. De functie is standaard uitgeschakeld.

- ***Bescherming expresberichten inschakelen*** – Schakel dit selectievakje in als u wilt controleren of de communicatie via expresberichten (bijvoorbeeld via *ICQ, MSN Messenger, ...*) vrij is van virussen.

- ***Geavanceerde instellingen***... – Klik op de koppeling als u het desbetreffende dialoogvenster met geavanceerde instellingen van **AVG Anti-Virus 2012** wilt weergeven. In dat dialoogvenster kunt u de configuratiedetails van het onderdeel bewerken. Wij wijzen u er echter op dat de standaardconfiguratie van alle onderdelen zo is afgestemd dat **AVG Anti-Virus 2012** optimale prestaties en een maximale beveiliging biedt. Het wordt aangeraden om de standaardconfiguratie te behouden, tenzij u een zeer goede reden hebt om dat niet te doen.

Knoppen

U kunt in dit dialoogvenster gebruikmaken van de volgende knoppen:

- ***Uitzonderingen beheren*** – Hiermee opent u een dialoogvenster met de naam Resident Shield - Uitzonderingen. Het dialoogvenster is tevens toegankelijk via het hoofdmenu, wanneer u Geavanceerde instellingen / Antivirus / Resident Shield / Uitzonderingen *kiest (zie het desbetreffende hoofdstuk voor een gedetailleerde beschrijving)*. U kunt binnen dit dialoogvenster bestanden en mappen opgeven die bij Resident Shield-scans moeten worden uitgesloten. Het wordt met klem aangeraden om geen mappen en bestanden over te slaan, tenzij dit absoluut noodzakelijk is. Dit dialoogvenster bevat de volgende knoppen:

  - *Pad toevoegen* – Hiermee kunt u een directory *(of directory's)* opgegeven die moeten worden uitgesloten bij het scannen door deze in de navigatiestructuur van de lokale schijf stuk voor stuk te selecteren.

  - *Bestand toevoegen* – Hiermee kunt u bestanden opgeven die moeten worden uitgesloten bij het scannen door deze in de navigatiestructuur van de lokale schijf stuk voor stuk te selecteren.

  - *Onderdeel bewerken* – Hiermee kunt u het opgegeven pad naar een geselecteerd bestand of een geselecteerde map bewerken.

  - *Onderdeel verwijderen* – Hiermee kunt u het pad naar een geselecteerd item in de lijst verwijderen.

- ***Wijzigingen opslaan*** – Hiermee kunt u alle wijzigingen in de instellingen van het onderdeel opslaan die in dit dialoogvenster zijn aangebracht, waarna u terugkeert naar de hoofd gebruikersinterface van het **AVG Anti-Virus 2012** (*onderdelenoverzicht*).

- ***Annuleren*** - Hiermee annuleert u alle wijzigingen in de instellingen van het onderdeel die u in dit dialoogvenster hebt aangebracht Er worden geen wijzigingen opgeslagen. U keert

terug naar de hoofd gebruikersinterface van **AVG Anti-Virus 2012** *het onderdelenoverzicht*.

6.1.5. Detecties door Resident Shield

Bedreiging gedetecteerd!

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 dit waarschuwingsvenster staan gegevens over het bestand dat is gedetecteerd als geïnfecteerd (*Bestandsnaam*), de naam van de gedetecteerde infectie (*De naam van de bedreiging*) en een koppeling naar de Virusencyclopedie met gedetailleerde informatie over het gedetecteerde virus, indien bekend (*Meer informatie*).

Vervolgens moet u bepalen, welke actie er moet worden uitgevoerd. Er zijn verscheidene opties beschikbaar. ***Welke knoppen beschikbaar zijn, is afhankelijk van de omstandigheden (het soort bestand dat is geïnfecteerd, de locatie van het bestand, enzovoort).***

- ***Bedreiging verwijderen als Power User*** – schakel dit selectievakje in als u denkt niet voldoende rechten te hebben om de bedreiging als gewoon gebruiker te verwijderen. Power Users hebben uitgebreide toegangsrechten en als de bedreiging zich in een bepaalde systeemmap bevindt, moet u dit vak misschien gebruiken om de bedreiging met succes te verwijderen.

- ***Herstellen*** – deze knop wordt alleen weergegeven als de gedetecteerde infectie kan worden hersteld. In dat geval wordt de infectie uit het bestand verwijderd en het bestand in zijn oorspronkelijke staat hersteld. Als het bestand zelf een virus is, kunt u het met deze functie verwijderen (*dat wil zeggen: verplaatsen naar de map Quarantaine*)

- ***Naar quarantaine verplaatsen*** – het virus zal naar de map Quarantaine

- ***Ga naar bestand*** – u wordt verwezen naar de exacte locatie van het verdachte object (*er*

wordt een nieuw Verkennervenster geopend)

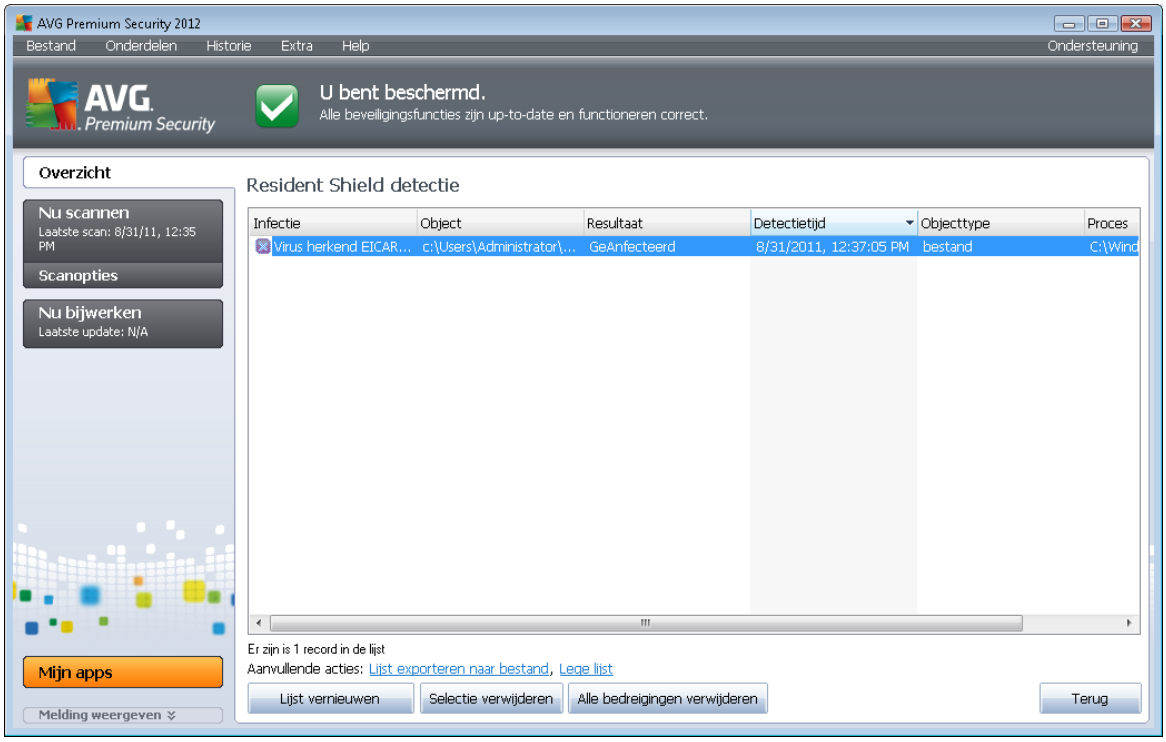
- ***Negeren*** – we raden u met nadruk aan deze optie NIET te kiezen tenzij u een heel goede reden hebt om dat wel te doen!

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

Onder in het dialoogvenster staat de koppeling ***Details weergeven*** – de koppeling opent een pop-upvenster met gedetailleerde informatie over het proces dat werd uitgevoerd op het moment dat de infectie werd gedetecteerd, en de identificatie van het proces.

Overzicht van bedreigingen die Resident Shield heeft gedetecteerd

Het totale overzicht van alle bedreigingen die Resident Shield heeft gedetecteerd, is te vinden in het dialoogvenster ***Resident Shield detectie*** dat u opent door het menu Historie / Resident Shield detectie 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 erboven 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*** gedetecteerde items vernieuwd. Als u op de knop ***Terug*** klikt, keert u terug naar het AGV-hoofddialoogvenster (*onderdelenoverzicht*).

6.2. LinkScanner

LinkScanner beschermt u tegen het toenemende gevaar van kortstondige bedreigingen op internet. Deze bedreigingen kunnen zich op elk type website verbergen, of het nu een website van de overheid, van een bekend merk of een klein bedrijf betreft, en zijn zelden langer dan 24 uur op dezelfde site aanwezig. ***LinkScanner*** analyseert alle pagina's die zijn gekoppeld aan de webpagina die u bezoekt en zorgt zo voor realtime beveiliging op het enige moment dat telt – het moment dat u op het punt staat op een koppeling te klikken.

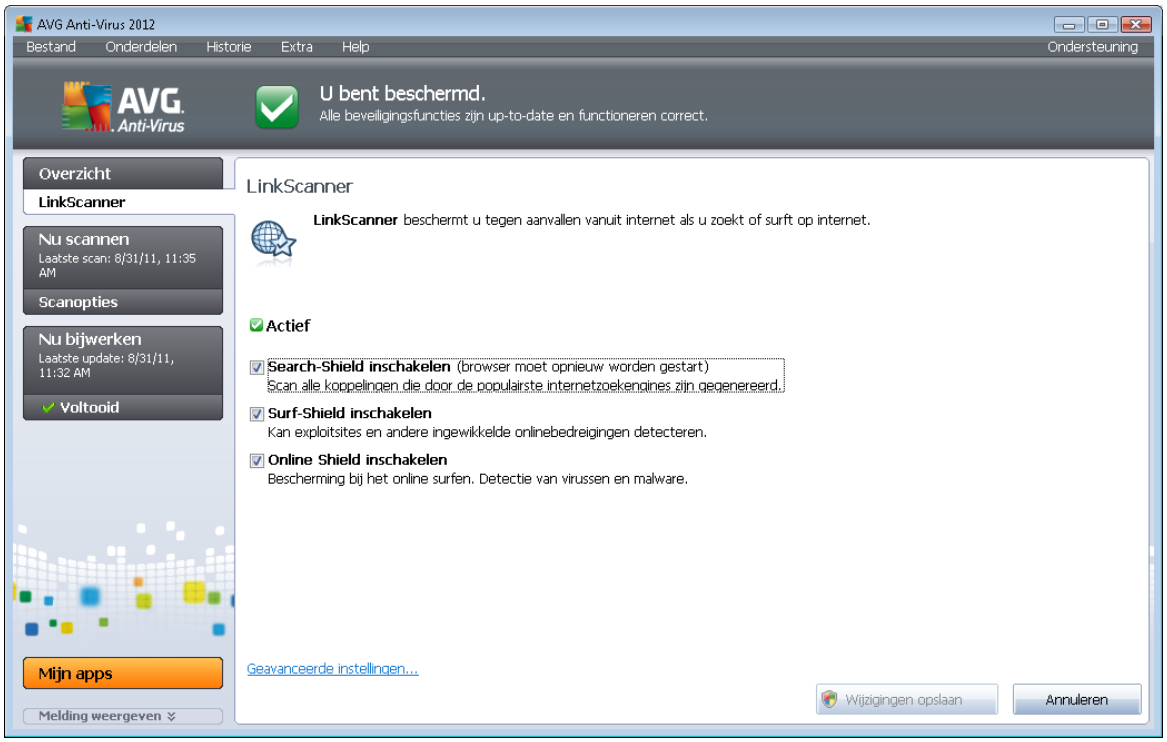
LinkScanner is niet bedoeld voor het beveiligen van serverplatforms.

De ***LinkScanner***-technologie omvat uit de volgende hoofdfuncties:

- Search-Shield bevat een lijst met websites (URL-adressen) waarvan bekend is dat deze gevaarlijk zijn. Wanneer u zoekt met Google, Yahoo!, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask en Seznam, worden alle zoekresultaten gecontroleerd op basis van deze lijst en wordt er een beoordelingspictogram weergegeven *(voor Yahoo! wordt alleen een pictogram weergegeven als het oordeel "website met exploit" is)*.
- Surf-Shield scant de inhoud van webpagina's die u bezoekt, ongeacht het adres van de website. Als een website niet door Search-Shield *wordt gedetecteerd (bijvoorbeeld wanneer er een nieuwe schadelijke website is gemaakt of wanneer een eerder veilige website nu malware bevat)*, wordt deze gedetecteerd en geblokkeerd door Surf-Shield wanneer u deze website probeert te bezoeken.
- Online Shield biedt realtime beveiliging tijdens het surfen op internet. Deze software scant de inhoud van bezochte webpagina's en eventueel aanwezige bestanden die daarin zijn opgenomen voordat deze in de webbrowser wordt weergegeven en naar uw computer worden gedownload. Online Shield detecteert viruses en spyware die zijn opgenomen in de pagina die u wilt bezoeken en stopt het downloaden onmiddellijk, zodat geen enkele bedreiging uw computer ooit kan bereiken.

6.2.1. LinkScanner-interface

Het hoofddialoogvenster van het onderdeel LinkScanner biedt een beknopte beschrijving van de functionaliteit van het onderdeel en in informatie over de huidige onderdeelstatus *(Actief)*:



In het onderste gedeelte van het dialoogvenster wordt een aantal basisopties voor het configureren van het onderdeel weergegeven:

- ***Search-Shield inschakelen*** - (*standaard ingeschakeld*): schakel dit selectievakje uitsluitend uit als u over een goede reden beschikt om de Search Shield-functionaliteit uit te schakelen.
- ***Surf-Shield inschakelen*** - (*standaard ingeschakeld*): actieve (*realtime*) beveiliging tegen websites waarbij er sprake is van exploits op het moment dat deze worden geopend. 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*).
- ***Online Shield inschakelen*** - (*standaard ingeschakeld*): webpagina's die u wilt openen, worden gescand op mogelijke virussen en spyware. Als deze worden gedetecteerd, wordt het downloaden onmiddellijk gestopt, zodat geen enkele bedreiging uw computer ooit bereikt.

6.2.2. Detecties door Search-Shield

Als u op internet zoekt, terwijl ***Search-Shield*** is ingeschakeld, worden alle zoekresultaten van de belangrijkste zoekmachines zoals *Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg en SlashDot* gecontroleerd op gevaarlijke of

verdachte koppelingen. LinkScanner 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 uitsluitend naar veilige websites gaat.

Terwijl een koppeling op de pagina met resultaten wordt beoordeeld, staat bij die koppeling een pictogram 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 (*dit pictogram wordt niet weergegeven bij veilige zoekresultaten van Yahoo! JP-zoekresultaten*.

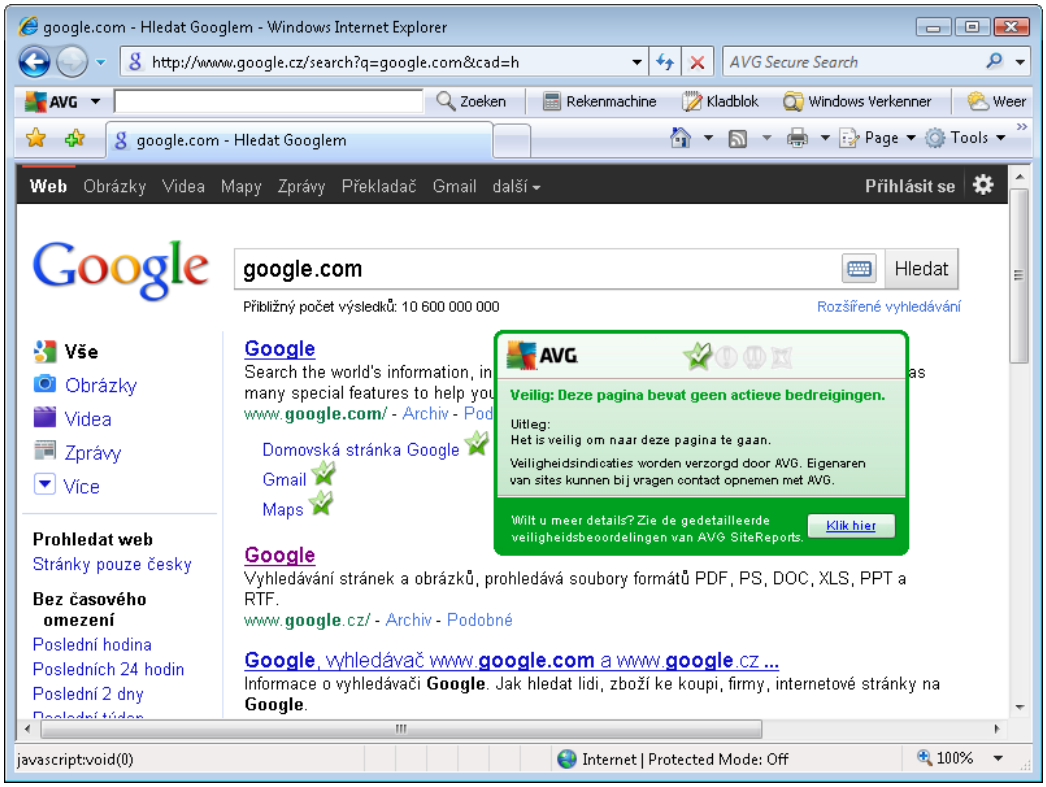
De gekoppelde pagina bevat geen bedreigingen, maar is enigszins verdacht (*of van twijfelachtige oorsprong of strekking en daarom niet geschikt voor e-shopping en dergelijke.*).

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.

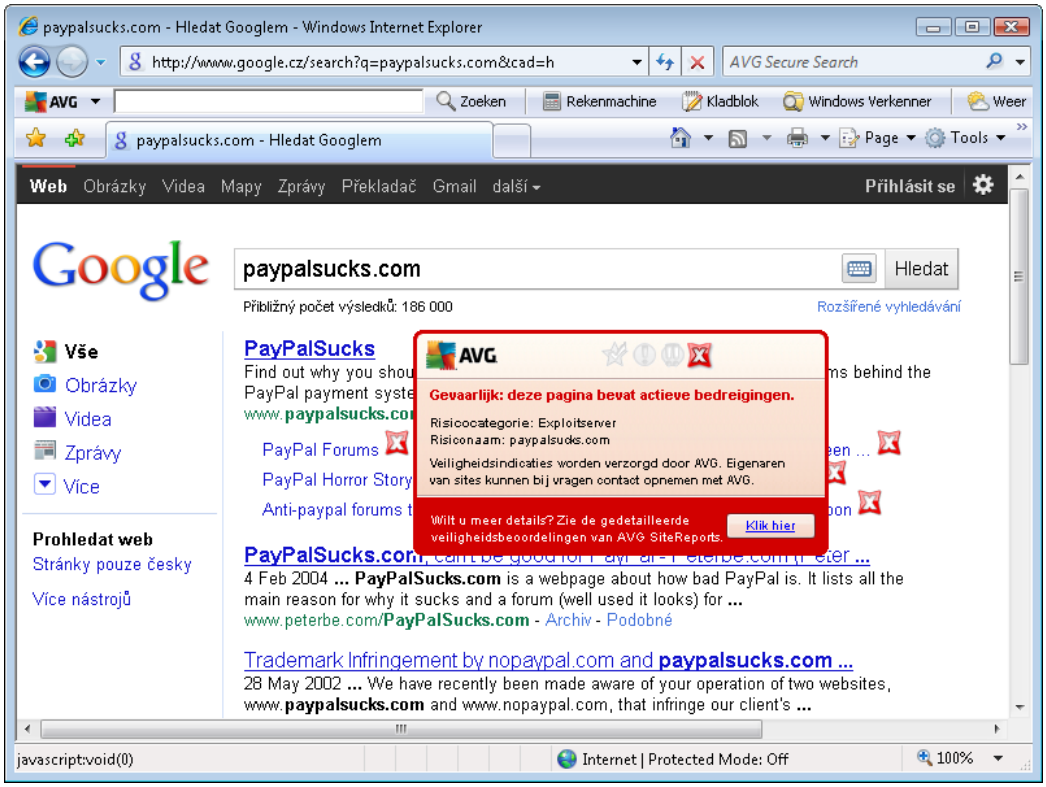
Als u de muisaanwijzer op een pictogram plaatst, worden details van de desbetreffende koppeling weergegeven. Er wordt ook extra informatie gegeven over de bedreiging (*als die er is*):



6.2.3. Detecties door 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 LinkScanner verhinderen dat uw webbrowser gevaarlijke webpagina's met exploits of andere serieuze bedreigingen weergeeft.

Als u wordt geconfronteerd met een schadelijke website, wordt u door LinkScanner gewaarschuwd via een soortgelijk scherm als het volgende:



Het openen van een dergelijke website is zeer gevaarlijk en wordt afgeraden.

6.2.4. Detecties door Online Shield

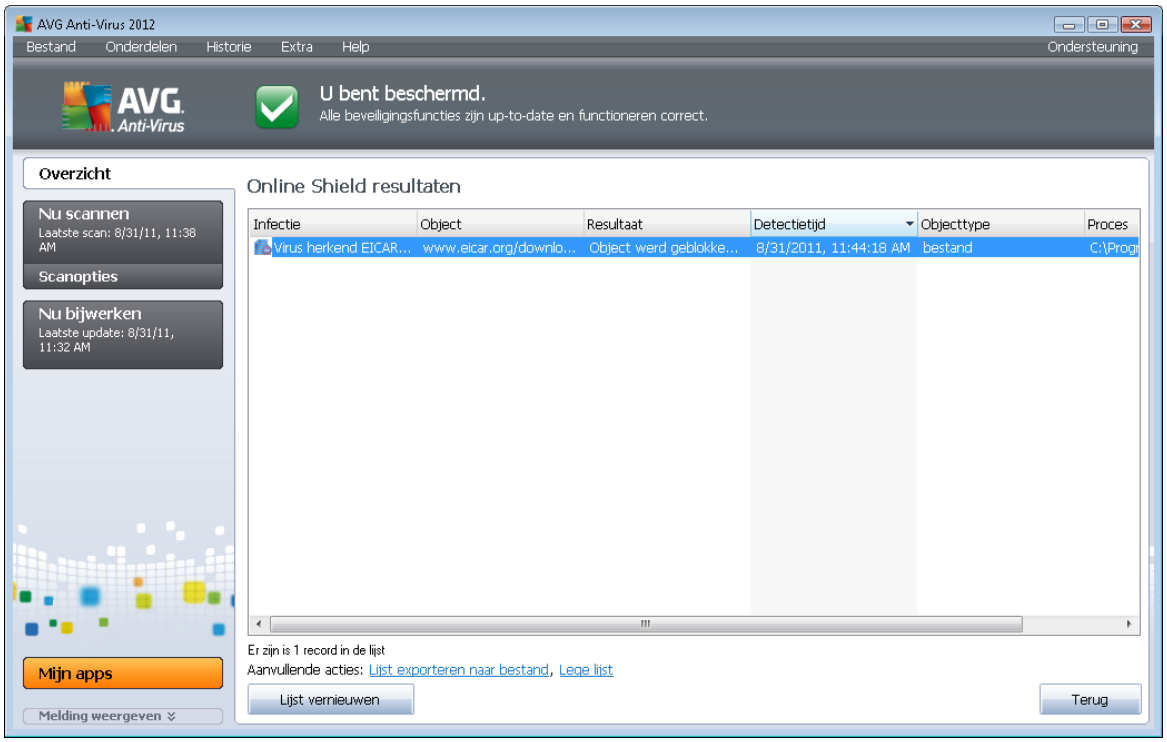
Online Shield scant de inhoud van bezochte webpagina's en eventuele bestanden die daarvan deel uitmaken zelfs voordat deze worden weergegeven in uw webbrowser of worden gedownload naar uw computer. Als een bedreiging wordt gedetecteerd, wordt u meteen gewaarschuwd door het volgende dialoogvenster:

In dit waarschuwingsvenster staan gegevens over het bestand dat is gedetecteerd als geïnfecteerd (*Bestandsnaam*), de naam van de gedetecteerde infectie (*de naam van de bedreiging*) en een koppeling naar de Virusencyclopedie met gedetailleerde informatie over het gedetecteerde virus (*indien bekend*). Dit dialoogvenster heeft de volgende knoppen:

- ***Details weergeven*** – klik op de knop ***Details weergeven*** om een nieuw pop-upvenster te openen met informatie over het proces dat werd uitgevoerd op het moment dat de infectie is gedetecteerd en gegevens over dat proces.

- ***Sluiten*** – het waarschuwingsvenster sluiten.

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 op de menubalk 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 erboven 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

- ***Lijst vernieuwen*** - Hiermee werkt u de lijst met items bij die zijn gedetecteerd door ***Online Shield***
- ***Terug*** - Hiermee kunt u terugkeren naar het AVG-hoofddialoogvenster *(onderdelenoverzicht)*

6.3. E-mailbescherming

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.

Het onderdeel ***E-mail Protection*** is verantwoordelijk voor het scannen van elk e-mailbericht dat wordt verzonden of ontvangen. Telkens als er een virus in een e-mail wordt gedetecteerd, wordt dit onmiddellijk verwijderd en naar het item Quarantaine verplaatst. Het onderdeel kan ook bepaalde typen bijlagen bij e-mail filteren en een certificatietekst toevoegen aan infectievrije berichten. ***E-mail Protection*** bestaat uit de volgende twee hoofdfuncties:

- E-mailscanner
- Anti-Spam

6.3.1. E-mailscanner

Het onderdeel E-mailscanner scant automatisch binnenkomende en uitgaande e-mails. U kunt het gebruiken voor e-mailclients die geen eigen invoegtoepassing hebben voor AVG (*, maar ook voor het scannen van e-mail van e-mailclients die door AVG worden ondersteund met een specifieke invoegtoepassing, bijvoorbeeld Microsoft Outlook en The Bat*). Het is vooral bedoeld voor e-mailtoepassingen als Outlook Express, Mozilla, Incredimail, enz.

Bij de installatie van AVG worden er automatische servers gemaakt voor het controleren 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 de poorten 110 en 25 (*standaardpoorten voor het versturen/ontvangen van e-mails*).

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 map quarantaine. Vervolgens wordt het bericht doorgegeven aan 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*).

E-mailscanner is niet bedoeld voor serverplatforms.

6.3.2. Antispam

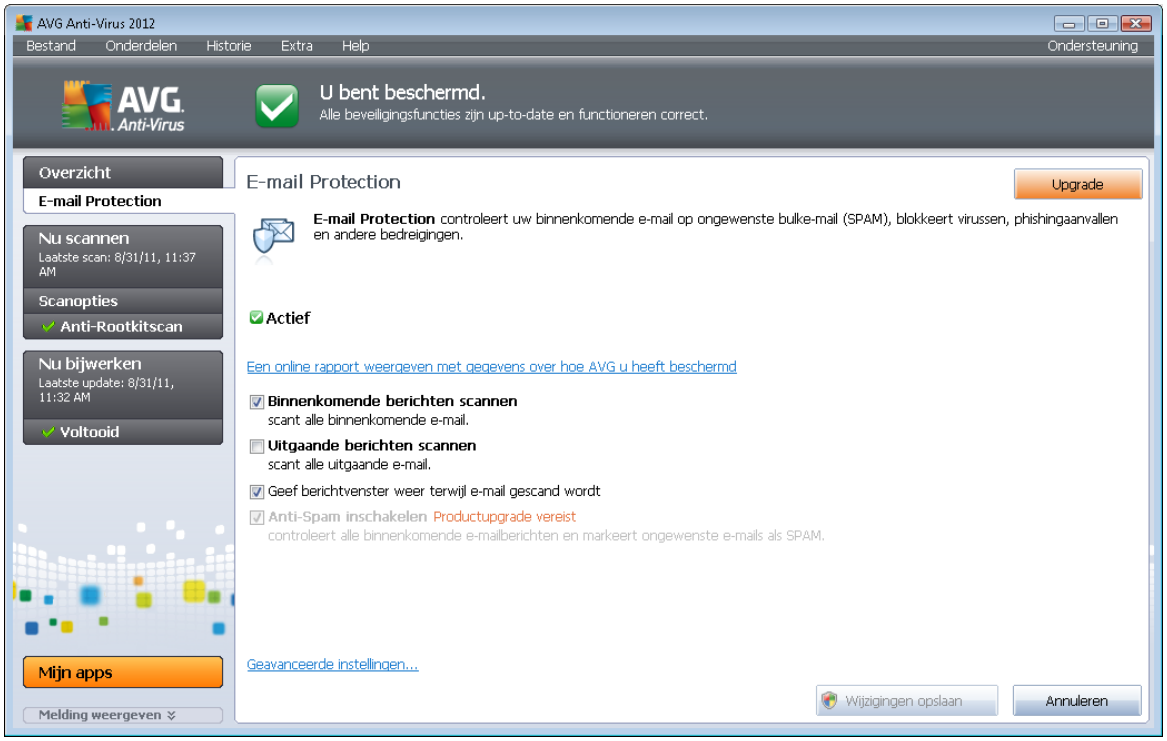
Hoe werkt Anti-Spam?

Anti-Spam controleert alle inkomende e-mailberichten en markeert ongewenste e-mails als spam. ***Anti-Spam*** kan het onderwerp wijzigen van e-mail (*die is herkend als spam*) door er een speciale teksttekenreeks aan toe te voegen. U kunt dan in uw e-mailclient de e-mails gemakkelijk filteren. ***Anti-Spam*** maakt gebruik van verschillende analysemethoden om de afzonderlijke e-mailberichten te verwerken. Dit biedt de best mogelijke bescherming tegen ongewenste e-mailberichten. ***Anti-Spam*** maakt voor spamdetectie gebruik van een database die regelmatig wordt bijgewerkt. U kunt ook RBL-servers opgeven (*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*).

Wat is 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.

6.3.3. E-mailbescherming-interface



Op het scherm van het onderdeel ***E-mail Protection*** staat een korte tekst met een beschrijving van de functie van het onderdeel en informatie over de huidige status (*E-mailscanner is actief).* Gebruik de koppeling ***Een online rapport weergeven met gegevens over hoe AVG u heeft beschermd*** als u gedetailleerde statistieken van **AVG Anti-Virus 2012** -activiteiten en -detecties wilt weergeven op een speciaal daartoe bestemde pagina van de AVG-website (http://www.avg.com/).

Basisinstellingen van E-mail Protection

In het dialoogvenster ***E-mail Protection*** kunt u tevens een aantal basisfuncties van de functionaliteit van het onderdeel instellen:

- ***Binnenkomende berichten scannen*** *(standaard ingeschakeld)* – Schakel dit selectievakje in om op te geven dat alle e-mailberichten die aan uw account zijn gericht, moeten worden gescand op virussen.
- ***Uitgaande berichten scannen*** *(standaard uitgeschakeld)* - Schakel dit selectievakje in om op te geven dat alle e-mailberichten die van uw account worden verzonden, moeten worden gescand op virussen.
- ***Geef berichtvenster weer terwijl e-mail gescand wordt*** *(standaard ingeschakeld)* – Schakel dit selectievakje in om te bevestigen dat u informatie wilt weergeven via een berichtvenster dat bij het AVG-pictogram in het systeemvak wordt weergegeven tijdens het scannen van uw e-mail.

De softwareleverancier heeft alle AVG-onderdelen ingesteld met het oog op optimale prestaties. Wijzig de configuratie van AVG niet, tenzij er een goede reden is om dat wel te doen. Wijzigingen in de instellingen dienen alleen te worden uitgevoerd door ervaren gebruikers. Als u de AVG-configuratie moet wijzigen, opent u het menu Extra / Geavanceerde instellingen en bewerkt u de AVG-configuratie in het dialoogvenster AVG Geavanceerde instellingen dat vervolgens wordt geopend.

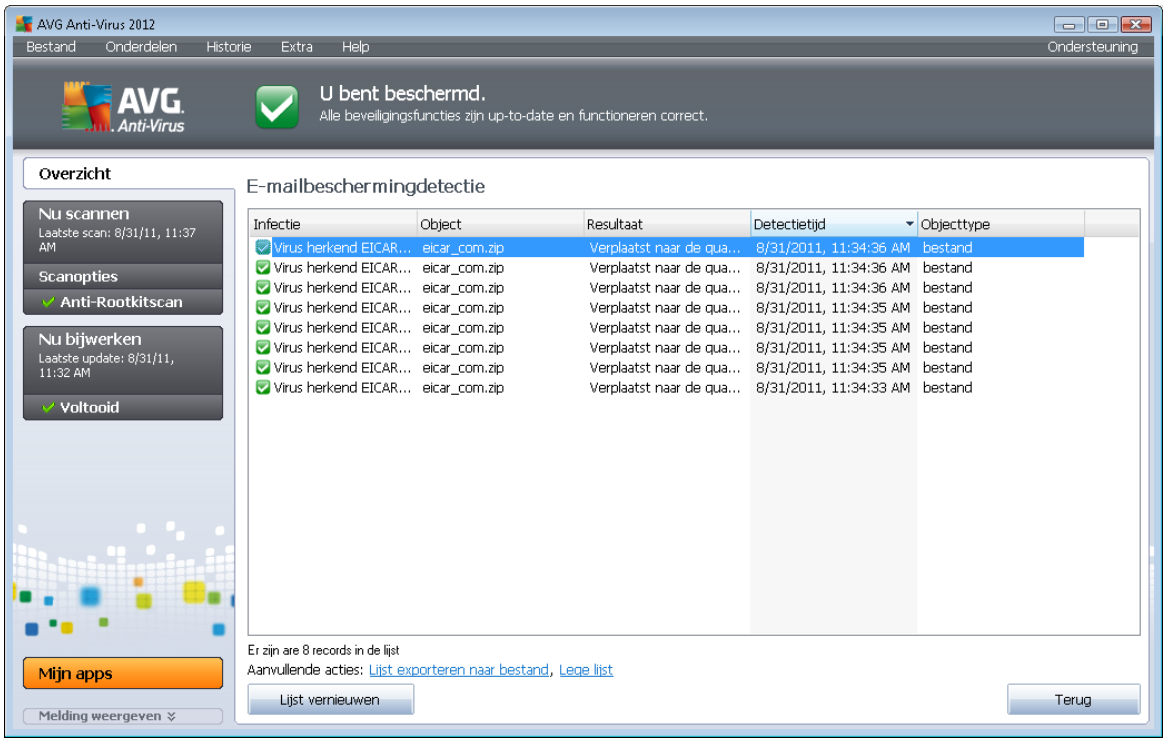
Als u het selectievakje ***Anti-Spam inschakelen*** inschakelt, wordt het filteren op de aanwezigheid van ongewenste berichten in uw binnenkomende e-mail geactiveerd. De Anti-Spam-service is niet beschikbaar in **AVG Anti-Virus 2012**. Deze service is uitsluitend toegankelijk in hogere AVG-edities. ***Bezoek de AVG-website (http://www.avg.com/) voor AVG-upgrade-informatie.***

Knoppen

De volgende knoppen zijn beschikbaar in het dialoogvenster ***E-mail Protection***:

- ***Wijzigingen opslaan*** – Druk op deze knop om de wijzigingen die u in het dialoogvenster hebt aangebracht op te slaan en toe te passen
- ***Annuleren*** – Druk op deze knop als u wilt terugkeren naar het AVG-hoofddialoogvenster (*onderdelenoverzicht*)

6.3.4. Detecties door E-mailbescherming



Het dialoogvenster ***E-mailscannerdetectie*** *(dat toegankelijk is via Historie / E-mailscannerdetectie)* 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 erboven 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*** – Hiermee kunt u de lijst met gedetecteerde bedreigingen bijwerken.
- ***Terug*** – Hiermee kunt u terugkeren naar het vorige weergegeven dialoogvenster.

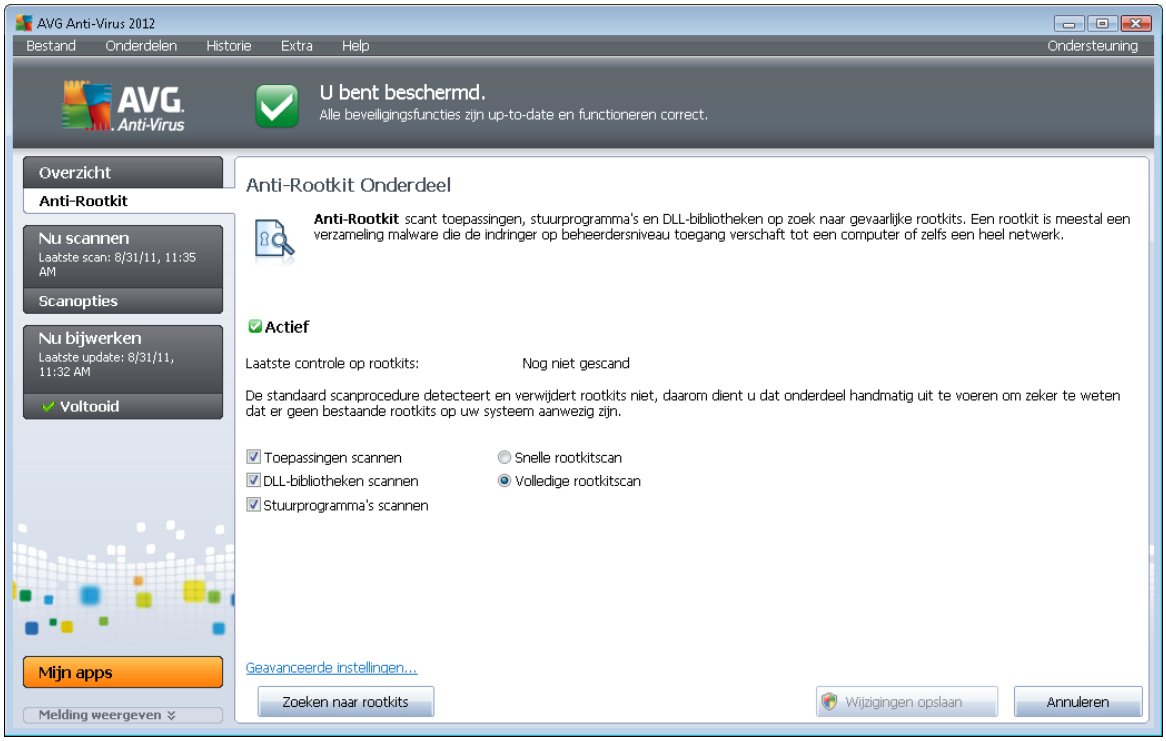
6.4. Antirootkit

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

Wat is een 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.

6.4.1. Antirootkit-interface



In het dialoogvenster ***Anti-Rootkit*** wordt een beknopte beschrijving gegeven van de functionaliteit van het onderdeel, wordt u geïnformeerd over de huidige status van het onderdeel *(Actief)* en wordt informatie weergegeven over de laatste keer dat de ***Anti-Rootkit***-test is gestart (***Laatste controle op rootkits***). In het dialoogvenster ***Anti-Rootkit*** kunt u bovendien via het menu Extra – Geavanceerde instellingen geavanceerde instellingen opgeven. Het dialoogvenster waarin u een geavanceerde configuratie kunt opgeven voor het onderdeel ***Anti-Rootkit*** wordt dan geopend.

De softwareleverancier heeft alle AVG-onderdelen ingesteld met het oog op optimale prestaties. Wijzig de configuratie van AVG niet, tenzij er een goede reden is om dat wel te doen. Wijzigingen in de instellingen dienen alleen te worden uitgevoerd door ervaren gebruikers.

Basisinstellingen van Anti-Rootkit

In het onderste gedeelte van het dialoogvenster kunt u een aantal basisfuncties voor het scannen op de aanwezigheid van rootkits instellen. 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:

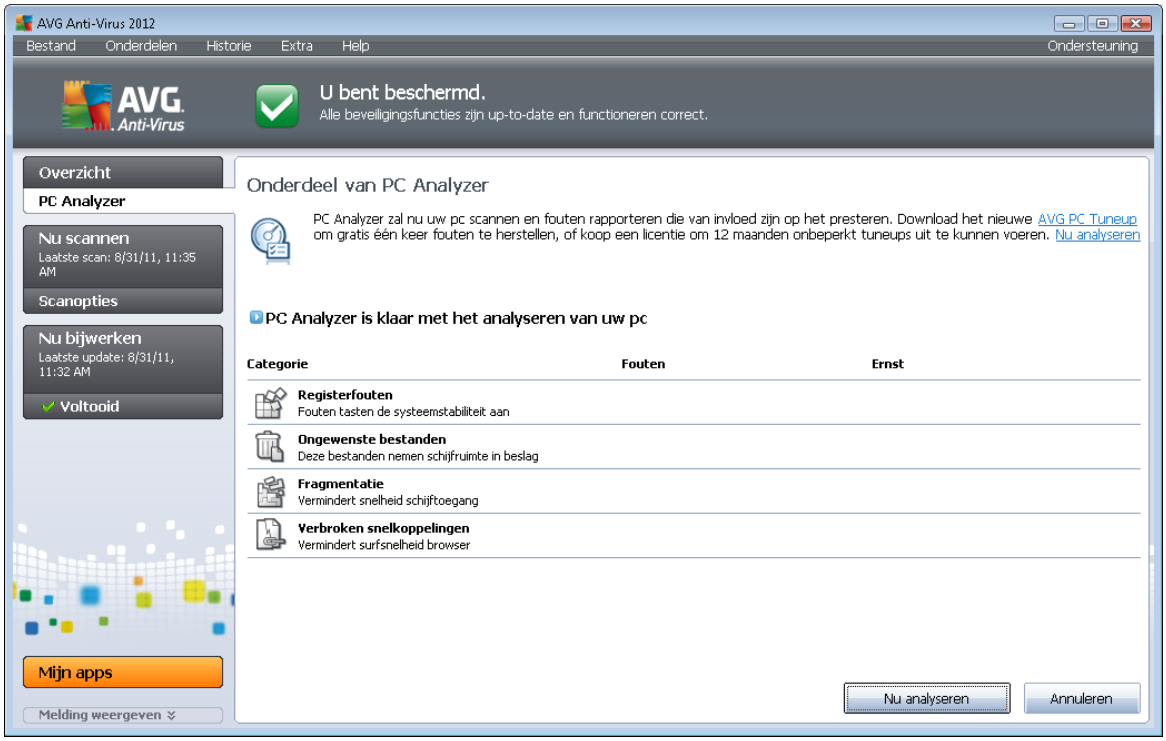
- ***Snelle rootkitscan*** - Hiermee scant u alle uitgevoerde processen, geladen stuurprogramma's en de systeemmap (*gewoonlijk c:\Windows*).
- ***Volledige rootkitscan*** - Hiermee scant u alle uitgevoerde processen, geladen stuurprogramma's, de systeemmap (*gewoonlijk c:\Windows*) en alle lokale schijven, (*waaronder USB-sticks. Diskettestations en cd-rom-stations worden niet gescand*).

Knoppen

- ***Zoeken naar rootkits*** - Aangezien de rootkitscan geen deel uitmaakt van de volledige computerscan, kunt u met behulp van deze knop de rootkitscan rechtstreeks vanuit de ***Anti-Rootkit***-interface starten.
- ***Wijzigingen opslaan*** - Druk op deze knop om alle wijzigingen die in deze interface zijn aangebracht op te slaan en terug te keren naar het AVG-hoofddialoogvenster (*onderdelenoverzicht*).
- ***Annuleren*** - Druk op deze knop als u wilt terugkeren naar het AVG-hoofddialoogvenster (*onderdelenoverzicht*) zonder dat eventueel aangebrachte wijzigingen worden opgeslagen.

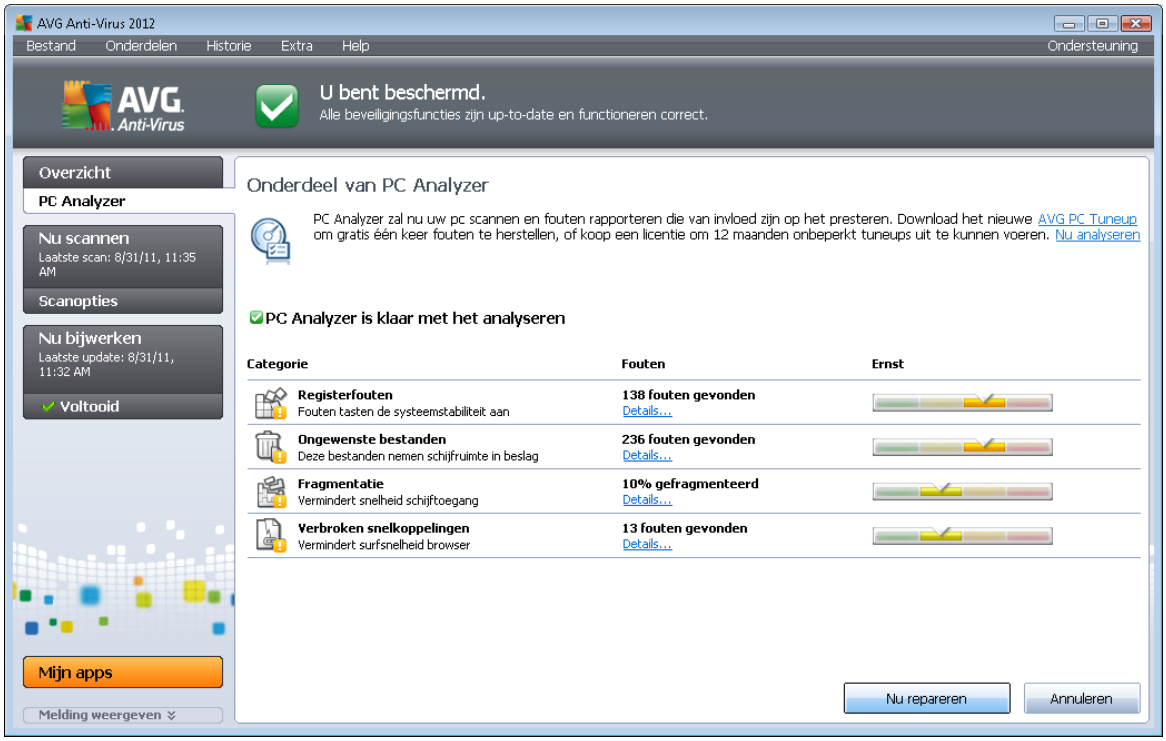
6.5. PC Analyzer

Het onderdeel ***PC Analyzer*** scant uw computer op systeemproblemen en laat op overzichtelijke manier zien op welke manier de prestaties in het geding zijn. De gebruikersinterface van het onderdeel bestaat uit een grafiek met vier lijnen die vier categorieën vertegenwoordigen: registerfouten, afvalbestanden, fragmentatie en verbroken koppelingen:



- ***Registerfouten*** – het aantal fouten in het Windows-register. Repareren van het Windows-register vergt vrij veel kennis; we raden u dan ook af daar zelf aan te beginnen.
- ***Afvalbestanden*** – het aantal bestanden dat waarschijnlijk overbodig is. Het gaat daarbij vooral om bestanden in tijdelijke mappen en in de Prullenbak.
- ***Fragmentatie*** berekent van het percentage van de vaste schijf dat is gefragmenteerd, dat wil zeggen dat het al lang in gebruik is, zodat de meeste bestanden nu in fragmenten verspreid zijn opgeslagen op verschillende delen van de vaste schijf. U kunt dat verhelpen met een programma voor het defragmenteren van de vaste schijf.
- ***Verbroken koppelingen*** – koppelingen die niet langer meer functioneren, die naar niet-bestaande locaties leiden, e.d. worden vermeld.

Klik op de knop ***Nu analyseren*** om de analyse te starten. De voortgang en de resultaten van de analyse worden in de grafiek weergegeven:



In het resultatenoverzicht staat het aantal systeemproblemen (***Fouten***) uitgesplitst naar categorie. De resultaten van de analyse worden bovendien grafisch weergegeven op een as in de kolom ***Ernst***.

Knoppen

- ***Nu analyseren*** (*weergegeven voor de start van de analyse*) – de analyse van de computer starten
- ***Nu repareren*** (*weergegeven na voltooiing van de analyse*) – hiermee kunt u de website van AVG (http://www.avg.com/, in het bijzonder de pagina met gedetailleerde en actuele informatie over het onderdeel ***PC Analyzer*** weergegeven
- ***Annuleren*** - Druk op deze knop als u het uitvoeren van de analyse wilt stoppen of als u wilt terugkeren naar het AVG-hoofddialoogvenster (*onderdelenoverzicht*) nadat de analyse is voltooid

6.6. Identity Protection

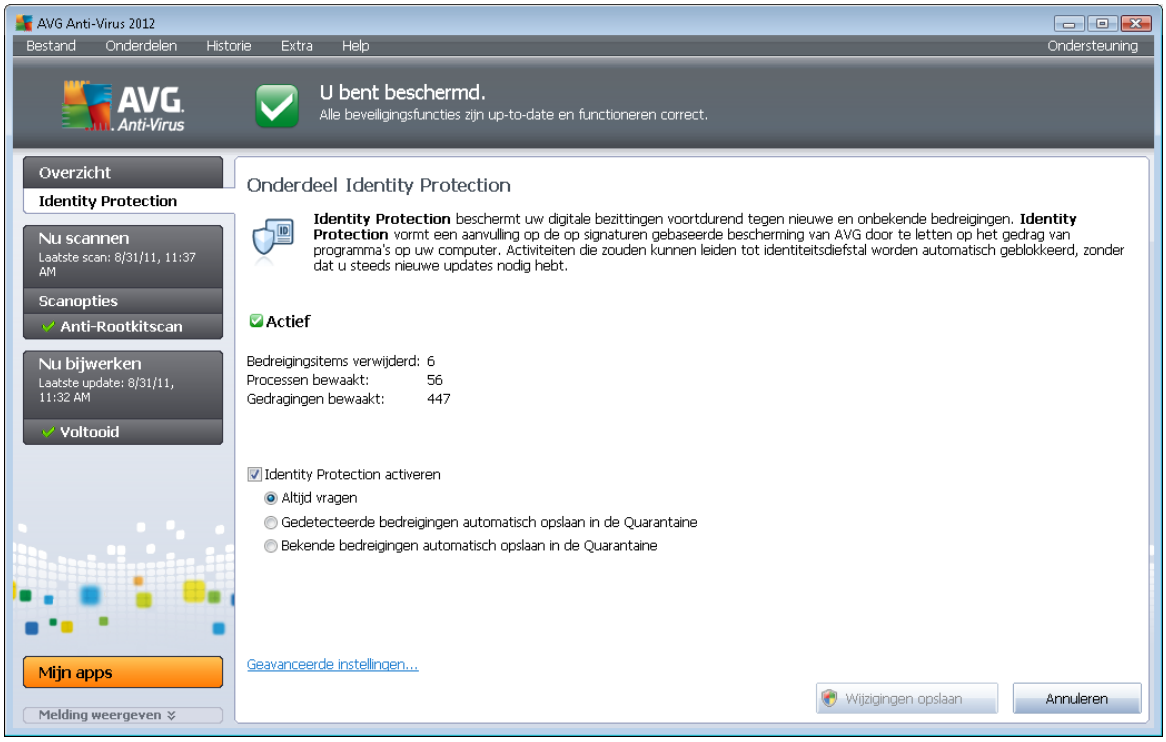
Identity Protection is een onderdeel voor anti-malware dat uw systeem beveiligt tegen allerlei vormen van malware (*zoals spyware, bots, identiteitsdiefstal, enzovoort*) via gedragsdetectietechnologieën. Dit onderdeel biedt u zonder enige vertraging beveiliging tegen nieuwe virussen. ***Identity Protection*** is gericht op het voorkomen van diefstal van uw wachtwoorden, bankrekeninggegevens, creditcardnummers en andere waardevolle persoonlijke digitale informatie door allerlei vormen van schadelijke software (*malware*) die uw pc bedreigen. Het product controleert of alle programma's die worden uitgevoerd op uw pc correct functioneren. ***Identity Protection*** detecteert en blokkeert verdacht gedrag en beveiligt uw computer tegen alle nieuwe schadelijke

software.

Het onderdeel ***Identity Protection*** beveiligt uw computer realtime tegen nieuwe en zelfs onbekende bedreigingen. Het onderdeel bewaakt alle (ook verborgen) processen en meer dan 285 verschillende gedragspatronen. Het onderdeel kan vaststellen of er iets schadelijks op uw systeem plaatsheeft. Daardoor kan het bedreigingen aan het licht brengen die zelfs nog niet zijn beschreven in de virusdatabases. Als een onbekend stukje code op uw computer arriveert, wordt dit onmiddellijk gecontroleerd op schadelijk gedrag en wordt dit item gevolgd. Als wordt geconstateerd dat het bestand schadelijk is, wordt dit door ***Identity Protection*** verwijderd naar de map Quarantaine en worden alle wijzigingen die in het systeem *zijn aangebracht, ongedaan gemaakt (code-injecties, wijzigingen van het register, het openen van poorten, enzovoort)*. U hoeft geen scan op te starten om beveiligd te zijn. De technologie is zeer proactief, behoeft nauwelijks te worden ge-updated, en is altijd waakzaam.

Identity Protection is een aanvullende beveiliging voor Anti-Virus. AVG raadt u aan om zowel een antivirusprogramma als Identity Protection te installeren, zodat uw PC volledig is beveiligd.

6.6.1. Identiteitsbescherming-interface



Het dialoogvenster ***Identity Protection*** biedt een beknopt overzicht van de basisfunctionaliteit en de status *(Actief)* van het onderdeel, evenals een aantal statistische gegevens:

- ***Bedreigingen verwijderd*** – het aantal toepassingen dat is gedetecteerd als malware en dat vervolgens is verwijderd
- ***Processen bewaakt*** – het aantal toepassingen dat op dat moment wordt uitgevoerd en wordt bewaakt door IDP

- ***Gedragingen bewaakt*** – het aantal specifieke acties dat in de bewaakte toepassingen wordt uitgevoerd

Basisinstellingen van E-mail Protection

In het onderste gedeelte van het dialoogvenster kunt u een aantal basisfuncties van de functionaliteit van het onderdeel instellen:

- ***Identity Protection activeren*** (*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:

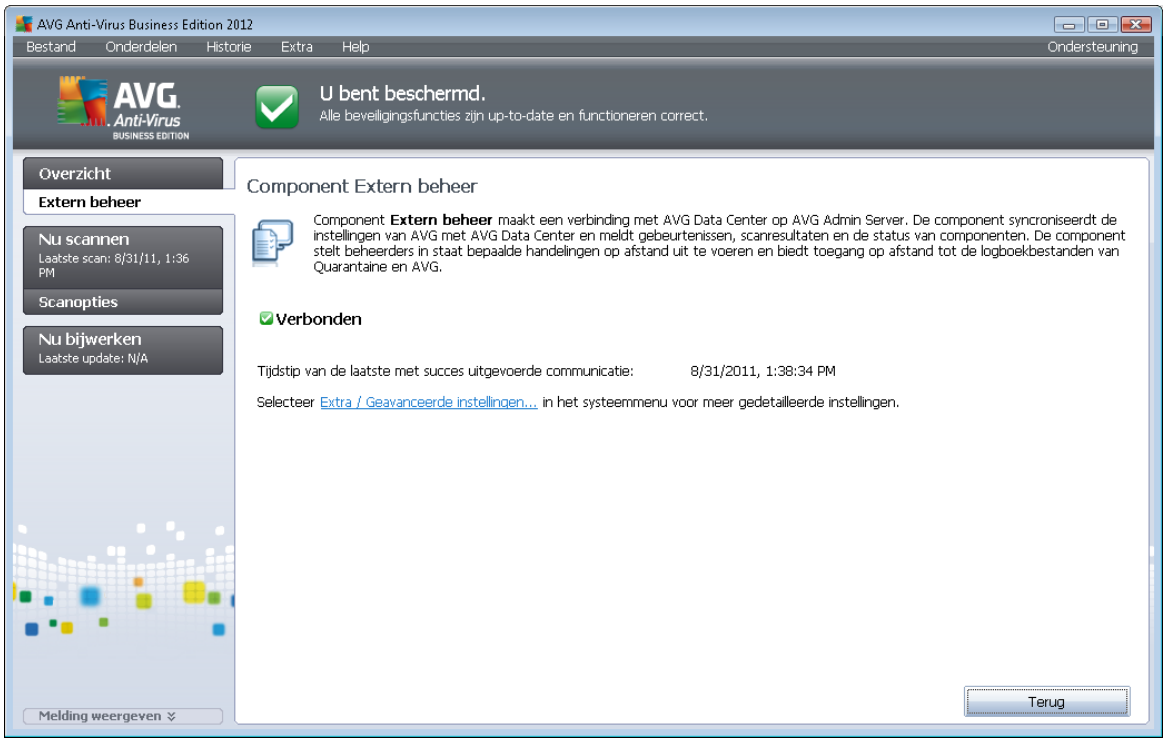
  - ***Altijd vragen*** – als een toepassing wordt herkend als malware, wordt u gevraagd of de toepassing moet worden geblokkeerd (*de optie is standaard ingeschakeld en we raden u aan deze niet te wijzigen, tenzij u een goede reden heeft om dit wel te doen*)
  - ***Gedetecteerde bedreigingen automatisch 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 aangebracht op te slaan en toe te passen
- ***Annuleren*** – druk op deze knop als u wilt terugkeren naar het AVG-hoofddialoogvenster (*onderdelenoverzicht*)

6.7. Extern beheer



Het onderdeel ***Extern beheer*** wordt uitsluitend weergegeven in de gebruikersinterface van **AVG Anti-Virus 2012** als u de zakelijke editie van het product *hebt geïnstalleerd (zie de informatie op het tabblad Versie in het dialoogvenster Informatie voor informatie over de licentie voor de installatie. U kunt dit dialoogvenster openen met behulp van het systeemmenu-item Ondersteuning)*. In het dialoogvenster ***Extern beheer*** wordt informatie weergegeven over of het onderdeel wel of niet actief is en of er een serververbinding aanwezig is. Alle instellingen van het onderdeel ***Extern beheer*** moeten worden opgegeven bij ***Geavanceerde instellingen / Extern beheer***.

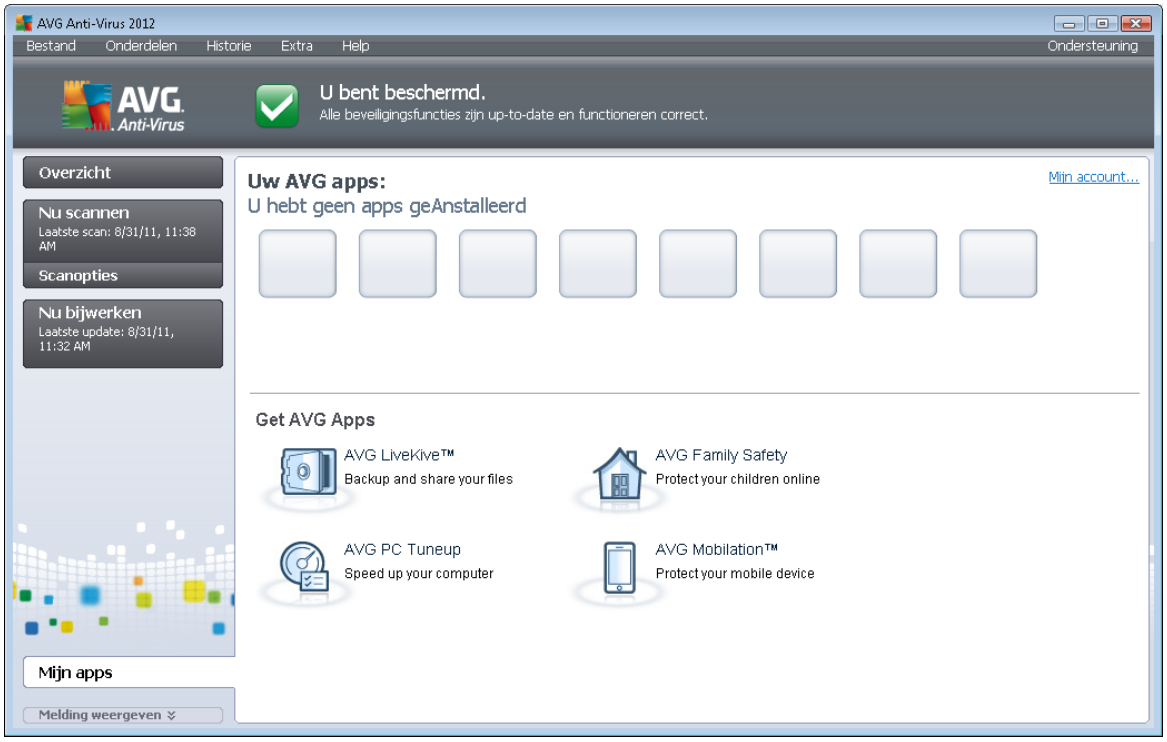
Raadpleeg de specifiek voor dit onderwerp ontwikkelde documentatie voor gedetailleerde informatie over de opties en functionaliteit van AVG Extern beheer. U kunt deze documentatie downloaden vanaf de AVG-website (http://www.avg.com/) in het gedeelte ***Support center / Downloaden / Documentatie***.

Knoppen

- ***Annuleren*** – druk op deze knop als u wilt terugkeren naar het AVG-hoofddialoogvenster (*onderdelenoverzicht*).

7. Mijn apps

Elk van de drie toepassingen LiveKive, Family Safety en PC Tuneup is verkrijgbaar als een zelfstandig AVG-product en een optioneel deel van uw **AVG Anti-Virus 2012**-installatie. In het dialoogvenster ***Uw AVG apps*** *(dat toegankelijk is via de knop Mijn apps in het AVG-hoofddialoogvenster)* wordt een overzicht weergegeven van toepassingen die al zijn geïnstalleerd en van toepassingen die optioneel kunnen worden geïnstalleerd:



7.1. LiveKive

LiveKive is speciaal bedoeld voor online gegevensback-ups op beveiligde servers. ***LiveKive*** maakt automatische back-ups van al uw bestanden, foto's en muziek op één veilige plaats, zodat u deze kunt delen met familie en vrienden en zodat deze bereikbaar zijn vanaf elk apparaat met toegang tot internet, waaronder iPhones en apparaten met Android. De ***LiveKive***-functies omvatten:

- Veiligheidsmaatregelen op het moment dat uw computer en/of vaste schijf beschadigd raken
- Toegang tot uw gegevens vanaf elk apparaat dat verbonden is met internet
- Eenvoudig organiseren
- Delen met iedereen die u autoriseert

Bezoek voor gedetailleerde informatie de bijbehorende AVG-webpagina. U kunt vanaf deze pagina ook het onderdeel downloaden. U kunt voor het weergeven van deze pagina gebruikmaken van de LiveKive-koppeling in het dialoogvenster Mijn apps.

7.2. Veiligheid voor het gezin

Family Safety helpt u uw kinderen beschermen tegen onbehoorlijke websites, media-inhoud en online zoekopdrachten en rapporteert over hun online activiteiten. U kunt voor elk van uw kinderen een passend niveau aan bescherming instellen en hen afzonderlijk volgen met behulp van unieke aanmeldingen.

Bezoek voor gedetailleerde informatie de bijbehorende AVG-webpagina. U kunt vanaf deze pagina ook het onderdeel downloaden. U kunt voor het weergeven van deze pagina gebruikmaken van de LiveKive-koppeling in het dialoogvenster Mijn apps.

7.3. PC TuneUp

De toepassing ***PC TuneUp*** is een geavanceerd hulpmiddel voor gedetailleerde analyses en correcties van het systeem op het gebied van de wijze waarop de snelheid en algehele prestaties van uw computer kunnen worden verbeterd. ***PC Tuneup*** omvat de volgende functies:

- Disk Cleaner - Hiermee verwijdert u overbodige bestanden die leiden tot tragere prestaties van uw computer.
- Disk Defrag - Hiermee defragmenteert u de schijfstations en optimaliseert u de plaatsing van systeembestanden.
- Registry Cleaner - Hiermee herstelt u registerfouten, zodat de stabiliteit van uw pc wordt bevorderd.
- Registry Defrag – Hiermee comprimeert u het register en verwijdert u ruimten die geheugen in beslag nemen.
- Disk Doctor – Hiermee kunt u naar beschadigde sectoren, verloren clusters en directoryfouten zoeken, zodat deze problemen kunnen worden hersteld.
- Internet Optimizer – Hiermee stemt u de algemene instellingen af op een specifieke internetverbinding.
- Track Eraser – Hiermee verwijdert u de geschiedenis van de computer en het internetgebruik.
- Disk Wiper – Hiermee wist u vrije ruimte op schijven, zodat het niet mogelijk is om vertrouwelijk gegevens terug te zetten.
- File Shredder – Hiermee verwijdert u geselecteerde bestanden op een schijf of USB-stick op een dergelijke wijze dat deze niet meer kunnen worden teruggezet.
- File Recovery – Hiermee kunt u per ongeluk van schijven, USB-sticks of camera's verwijderde bestanden terugzetten.
- Duplicate File Finder – Hiermee kunt u dubbele bestanden zoeken en verwijderen, zodat er geen schijfruimte wordt verspild.
- Services Manager – Hiermee kunt u overbodige services die uw computer trager maken,

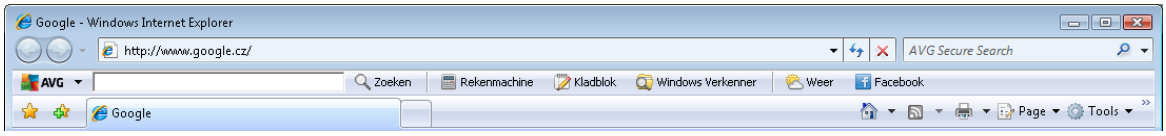
uitschakelen.

- Startup Manager – Hiermee kunt u programma's beheren die automatisch worden gestart tijdens het opstarten van Windows.
- Uninstall Manager – Hiermee kunt u de softwareprogramma's die u niet langer nodig hebt volledig verwijderen.
- Tweak Manager – Hiermee kunt u honderden verborgen Windows-instellingen afstemmen.
- Task Manager – Hiermee kunt u alle processen en services die worden uitgevoerd, weergeven, evenals alle vergrendelde bestanden.
- Disk Explorer – Hiermee kunt u weergeven welke bestanden op de computer de meeste ruimte in beslag nemen.
- Systeemgegevens - Hiermee kunt u gedetailleerde informatie weergeven over geïnstalleerde hardware en software.

Bezoek voor gedetailleerde informatie de speciale AVG-webpagina. U kunt het onderdeel via deze pagina onmiddellijk downloaden. U kunt hiertoe gebruikmaken van de PC Tuneup-koppeling in het dialoogvenster Mijn apps.

8. AVG Werkbalk Beveiliging

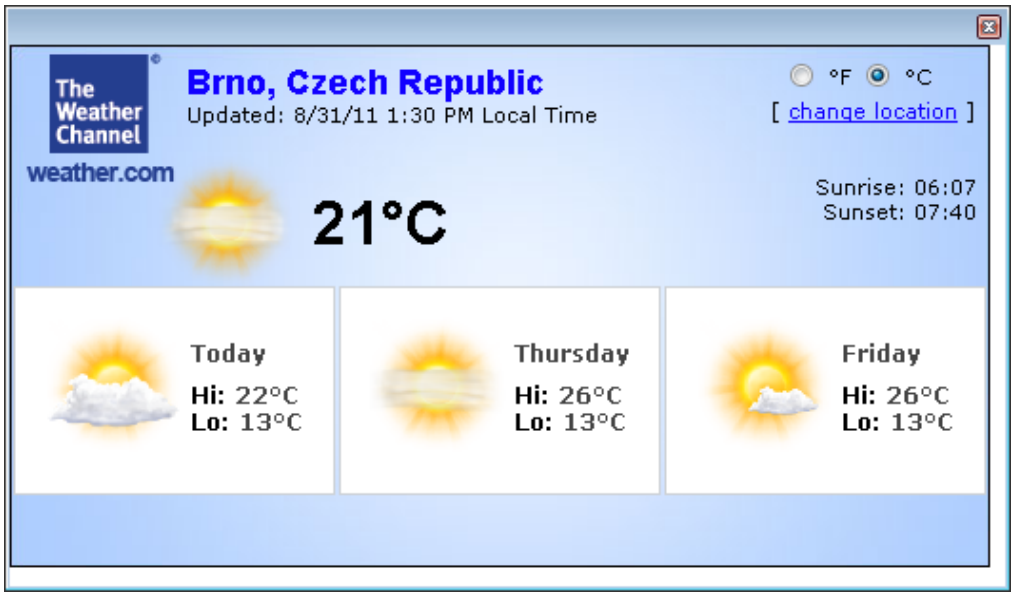
AVG Werkbalk Beveiliging is een hulpmiddel dat nauw samenwerkt met het onderdeel LinkScanner en dat tijdens het surfen op internet uw maximale beveiliging waarborgt. De installatie van ***AVG Werkbalk Beveiliging*** is binnen **AVG Anti-Virus 2012** optioneel. U wordt gedurende het installatieproces gevraagd of u het onderdeel wilt installeren. ***AVG Werkbalk Beveiliging*** is rechtstreeks beschikbaar in uw internetbrowser. Er wordt momenteel ondersteuning geboden voor de volgende internetbrowsers: Internet Explorer (*versie 6.0 en hoger*) en/of Mozilla Firefox (*versie 3.0 en hoger*). Er wordt geen ondersteuning geboden voor andere browsers *(wanneer u alternatieve internetbrowsers gebruikt, zoals Avant Browser, moet u rekening houden met onverwacht gedrag)*.



AVG Werkbalk Beveiliging bestaat uit de volgende onderdelen:

- ***Het AVG-logo*** met de vervolgkeuzelijst:
  - ***AVG Secure Search*** - U kunt rechtstreeks vanuit de ***AVG Werkbalk Beveiliging*** zoeken, dankzij het ***AVG Secure Search***-programma. Alle zoekresultaten worden voortdurend gecontroleerd door de Search-Shield-service, zodat u zich online absoluut veilig kunt voelen.
  - ***Huidig bedreigingsniveau*** - Hiermee opent u de webpagina van het viruslab met een grafische weergave van het huidige bedreigingsniveau op het web.
  - ***AVG Threat Labs*** - Hiermee opent u de pagina voor ***siterapporten*** op de AVG-website (http://www.avg.com/). U kunt op deze pagina op naam zoeken naar specifieke bedreigingen en gedetailleerde informatie over afzonderlijke bedreigingen weergeven.
  - ***Werkbalk Help*** - Hiermee opent u de online Help met Help-onderwerpen over de gehele functionaliteit van ***AVG Werkbalk Beveiliging***.
  - ***Productfeedback verzenden*** - Hiermee opent u een webpagina met een formulier dat u kunt invullen als u ons wilt voorzien van feedback over ***AVG Werkbalk Beveiliging***.
  - ***Info...*** - Hiermee opent u een nieuw venster met informatie over de huidige geïnstalleerde versie van ***AVG Werkbalk Beveiliging***.
- ***Zoekvak*** - Hiermee kunt u op internet zoeken met gebruik van ***AVG Werkbalk Beveiliging***, zodat u volledig veilig en comfortabel kunt zoeken, aangezien alle zoekresultaten honderd procent veilig zijn. Typ een trefwoord of zin in het zoekvak en druk op de knop ***Zoeken*** *(of op Enter)*. Alle zoekresultaten worden door de Search-Shield-service *voortdurend gecontroleerd (binnen het onderdeel LinkScanner)*.
- Snelkoppelingen voor snelle toegang tot deze toepassingen: ***Rekenmachine***, ***Kladblok***, ***Windows Verkenner***

- ***Weer*** – Deze knop opent een nieuw dialoogvenster met informatie over het huidige weer op uw locatie en de weersverwachting voor de komende twee dagen. Deze informatie wordt regelmatig bijgewerkt (om de 3-6 uur). U kunt in dit dialoogvenster handmatig de gewenste locatie instellen en u kunt instellen of u temperatuurinformatie wilt weergeven in graden Celsius of Fahrenheit.



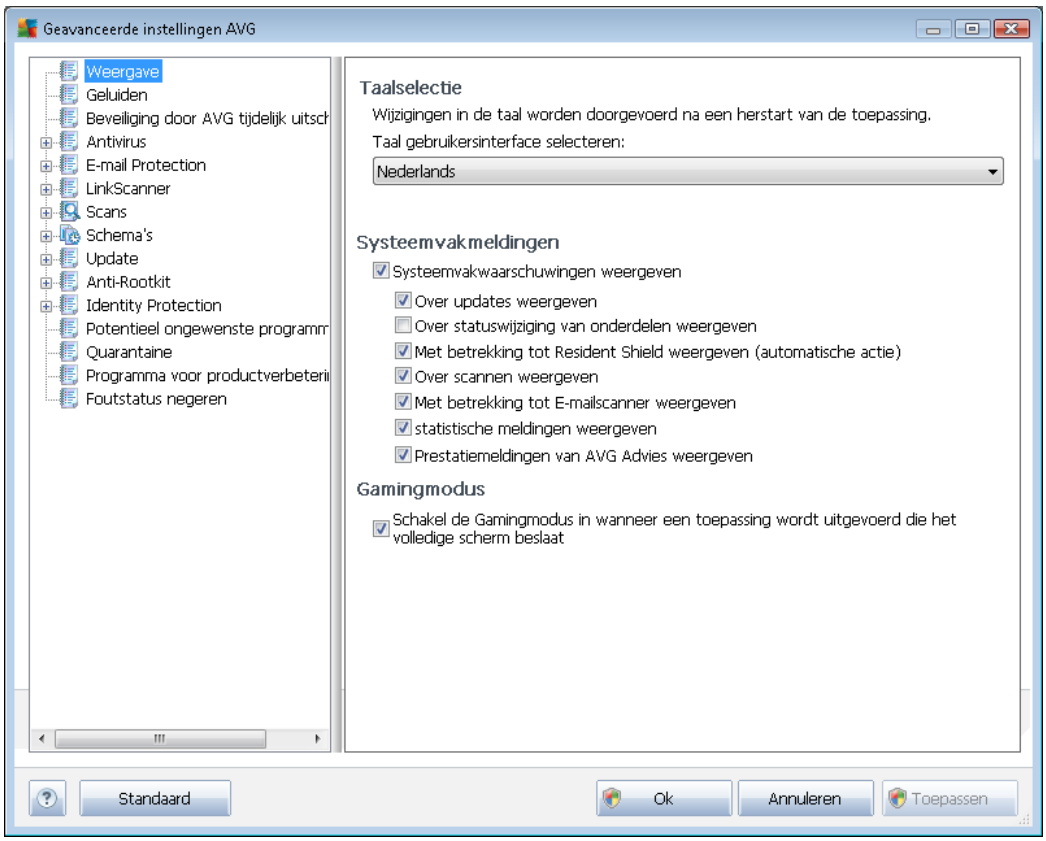
- ***Facebook*** – Deze knop maakt het mogelijk om rechtstreeks vanuit ***AVG Werkbalk Beveiliging*** verbinding te maken met sociale netwerk Facebook. *gedrag.*

9. AVG Geavanceerde instellingen

Het dialoogvenster voor een geavanceerde configuratie van **AVG Anti-Virus 2012** 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.

9.1. Weergave

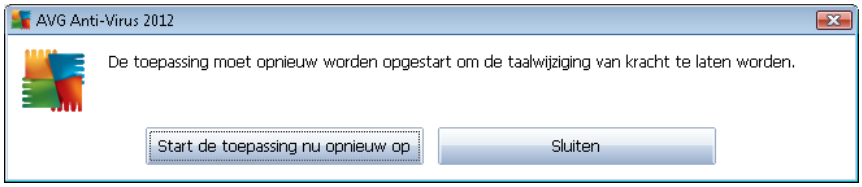
Het eerste onderdeel van de navigatiestructuur, ***Weergave***, verwijst naar de algemene instellingen van de **AVG Anti-Virus 2012**-gebruikersinterface en bevat een aantal basisopties die betrekking hebben op het gedrag van de toepassing:



Taalselectie

U kunt in de vervolgkeuzelijst in de sectie ***Taalselectie*** de gewenste taal kiezen. De geselecteerde taal wordt vervolgens gebruikt voor de gehele **AVG Anti-Virus 2012**-gebruikersinterface. De vervolgkeuzelijst bevat alleen de talen die u eerder tijdens het installatieproces hebt geïnstalleerd (*zie het hoofdstuk Aangepaste opties*) plus Engels (*Engels wordt standaard automatisch geïnstalleerd*). Als u het op een andere taal instellen van **AVG Anti-Virus 2012** wilt voltooien, moet u de toepassing opnieuw starten. Volg daartoe de volgende stappen:

- Selecteer in de vervolgkeuzelijst de gewenste taal voor de toepassing
- Bevestig uw keuze door op de knop ***Toepassen*** te klikken *(deze knop wordt in de rechterbenedenhoek van het dialoogvenster weergegeven)*
- Klik op de knop ***OK*** om te bevestigen
- Er wordt een nieuw dialoogvenster weergegeven met de vermelding dat voor het wijzigen van de taal van de toepassing opnieuw opstarten nodig is van **AVG Anti-Virus 2012**
- Druk op de knop ***De toepassing nu opnieuw starten*** om in te stemmen met het opnieuw opstarten van het programma en wacht totdat de taalwijzing van kracht wordt:



Systeemvakmeldingen

Deze sectie biedt u de mogelijkheid om de weergave van systeemmeldingen over de status van de **AVG Anti-Virus 2012**-toepassing te onderdrukken. Systeemmeldingen worden standaard weergegeven. Het wordt met klem aangeraden om deze configuratie te behouden. Systeemmeldingen informeren u bijvoorbeeld over het scanproces, het updateproces of een statuswijziging van een onderdeel van **AVG Anti-Virus 2012**. Het is belangrijk dat u aandacht aan deze meldingen besteedt.

Wanneer u echter om welke reden dan ook besluit dat u niet op deze wijze wilt worden geïnformeerd of dat u alleen bepaalde meldingen *(die betrekking hebben op een specifiek AVG Anti-Virus 2012-onderdeel)* wilt weergeven, kunt u uw voorkeuren instellen door de volgende opties in of uit te schakelen:

- ***Systeemvakwaarschuwingen weergeven*** *(standaard ingeschakeld)* - Standaard worden alle waarschuwingen weergegeven. Schakel dit selectievakje uit als u de weergave van alle systeemmeldingen volledig wilt uitschakelen. Als u de optie inschakelt, kunt u selecteren welke meldingen u wilt weergeven:
  - ***Systeemvakmeldingen over updates*** *weergeven (standaard ingeschakeld)* - Bepaal of informatie over **AVG Anti-Virus 2012** het starten, de voortgang en het voltooien van het updateproces moet worden weergegeven.
  - ***Systeemvakmeldingen over statuswijziging van onderdelen weergeven*** *(standaard uitgeschakeld)* – Bepaal of informatie over de activiteit/inactiviteit van een onderdeel of over een mogelijk probleem met het onderdeel moet worden weergegeven. Wanneer de foutstatus van een onderdeel wordt gerapporteerd, heeft deze optie hetzelfde effect als de informatieve functie van het systeemvakpictogram dat een probleem aangeeft met een **AVG Anti-Virus 2012**-onderdeel.

- ***Systeemvakmeldingen met betrekking tot Resident Shield weergeven (automatische actie)*** *(standaard ingeschakeld)* – Bepaal of u informatie over procedures voor het opslaan, kopiëren en openen van bestanden wilt weergeven of niet (*deze instelling wordt alleen weergegeven als de Resident Shield-optie Automatisch herstel is ingeschakeld*).

- ***Systeemvakmeldingen over scannen*** *weergeven (standaard ingeschakeld)* - Bepaal of u informatie over het automatisch starten van geplande scans, de voortgang en de resultaten wilt weergeven

- ***Systeemvakmeldingen met betrekking tot E-mailscanner weergeven*** *(standaard ingeschakeld)* – Bepaal of u informatie over het scannen van alle inkomende en uitgaande e-mailberichten wilt weergeven.

- ***Statistische meldingen weergeven*** *(standaard ingeschakeld)* – Zorg ervoor dat deze optie is ingeschakeld als u op een regelmatige basis statistische gegevensmeldingen wilt weergeven in het systeemvak.

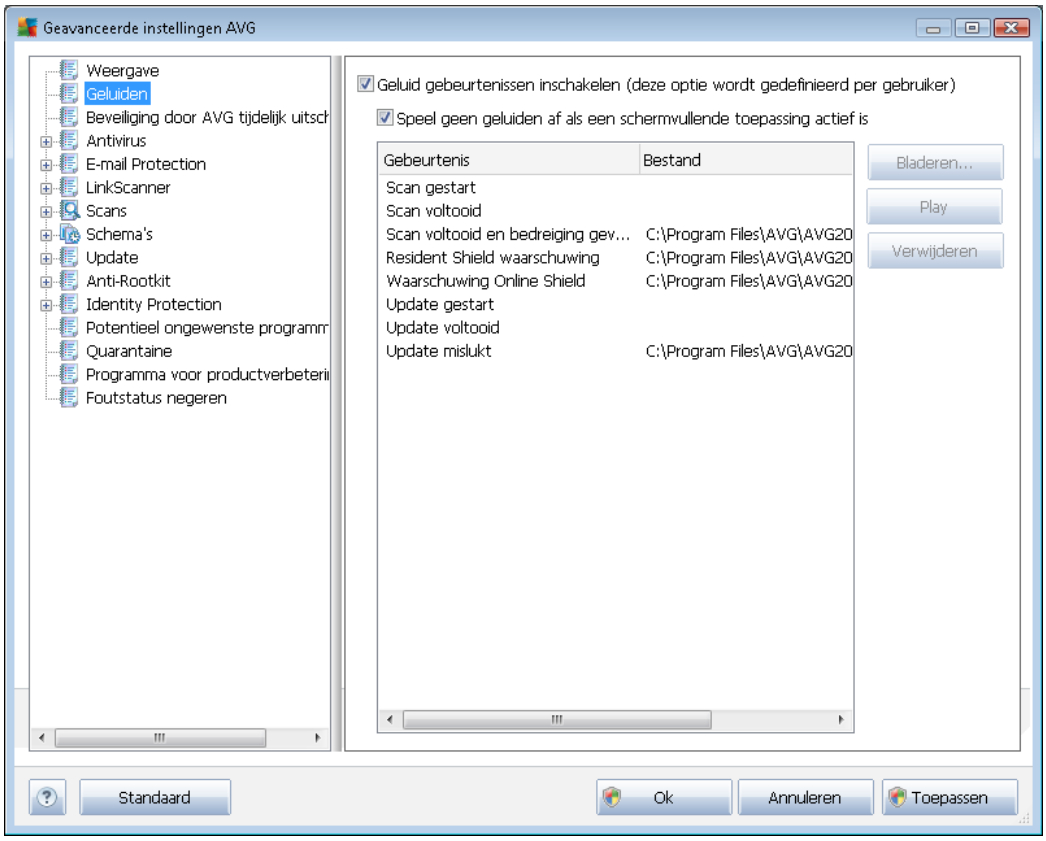
- ***AVG Advice-prestatiemeldingen weergeven*** *(standaard ingeschakeld)* - ***AVG Advice*** bewaakt de prestaties van de ondersteunde internetbrowsers *(Internet Explorer, Chrome, Firefox, Opera en Safari)* en informeert u wanneer uw browser de aanbevolen geheugenhoevoeelheid overschrijdt. In een dergelijke situatie lopen de prestaties van de computer mogelijk in belangrijke mate terug en is het raadzaam om uw internetbrowser opnieuw te starten, zodat de processen worden versneld. Zorg ervoor dat de optie ***AVG Advice-prestatiemeldingen weergeven*** is ingeschakeld als u wilt worden geïnformeerd.

Gamingmodus

Deze AVG-functie is ontworpen voor schermvullende toepassingen, waarbij AVG-meldingen (*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*).

9.2. Geluiden

In het dialoogvenster ***Geluiden*** kunt u instellen of u via een geluidssignaal in kennis gesteld wilt worden van specifieke acties van **AVG Anti-Virus 2012**:



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

Knoppen

- ***Bladeren*** – Gebruik nadat u de gewenste gebeurtenis hebt geselecteerd in de lijst de knop ***Bladeren*** om een geluidsbestand op uw schijf te selecteren, zodat u dit kunt toewijzen. *(Houd er rekening mee dat er momenteel uitsluitend ondersteuning wordt geboden voor *.wav-geluiden.)*

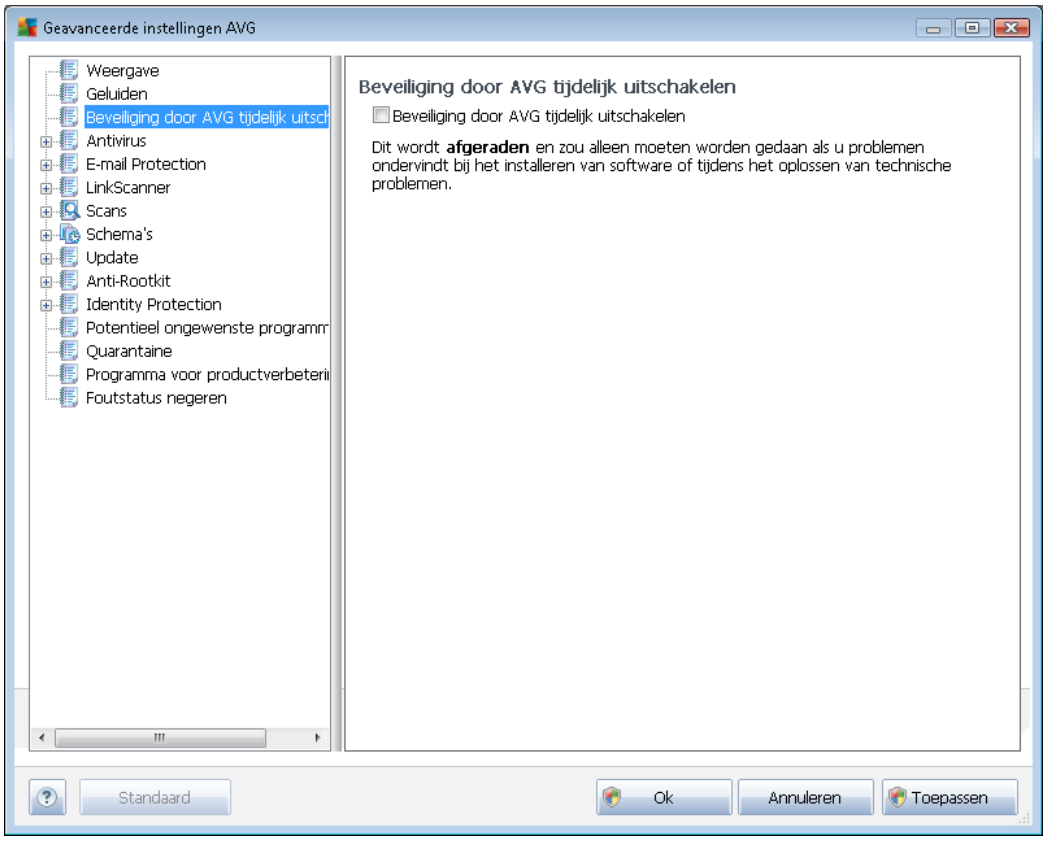
- ***Afspelen*** – Als u het geselecteerde geluid wilt beluisteren, markeert u de gebeurtenis in de lijst en drukt u op de knop ***Afspelen***.

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

9.3. Beveiliging door AVG tijdelijk uitschakelen

In het dialoogvenster ***Beveiliging door AVG tijdelijk uitschakelen*** kunt u de volledige bescherming door **AVG Anti-Virus 2012** in één keer uitschakelen.

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



In de meeste gevallen is het ***niet nodig*** om **AVG Anti-Virus 2012** uit te schakelen voordat u nieuwe software of stuurprogramma's installeert, zelfs niet als het installatieprogramma of de softwarewizard voorstelt eerst lopende programma's en toepassingen uit te schakelen om ervoor te zorgen dat er zich geen ongewenste onderbrekingen voordoen tijdens het installatieproces. Als u tijdens de installatie daadwerkelijk op problemen mocht stuiten, kunt u eerst proberen om de residente beveiliging uit te schakelen (*Resident Shield uitschakelen*). Als u **AVG Anti-Virus 2012** tijdelijk moet uitschakelen, moet u de beveiliging zo snel mogelijk opnieuw inschakelen. Uw computer is kwetsbaar en kan worden aangevallen als u verbonden bent met internet of een netwerk gedurende de tijd dat uw beveiliging is uitgeschakeld.

De AVG-beveiliging tijdelijk uitschakelen

- Schakel het selectievakje ***Beveiliging door AVG tijdelijk uitschakelen*** in en bevestig uw

keuze door op de knop ***Toepassen*** te drukken.

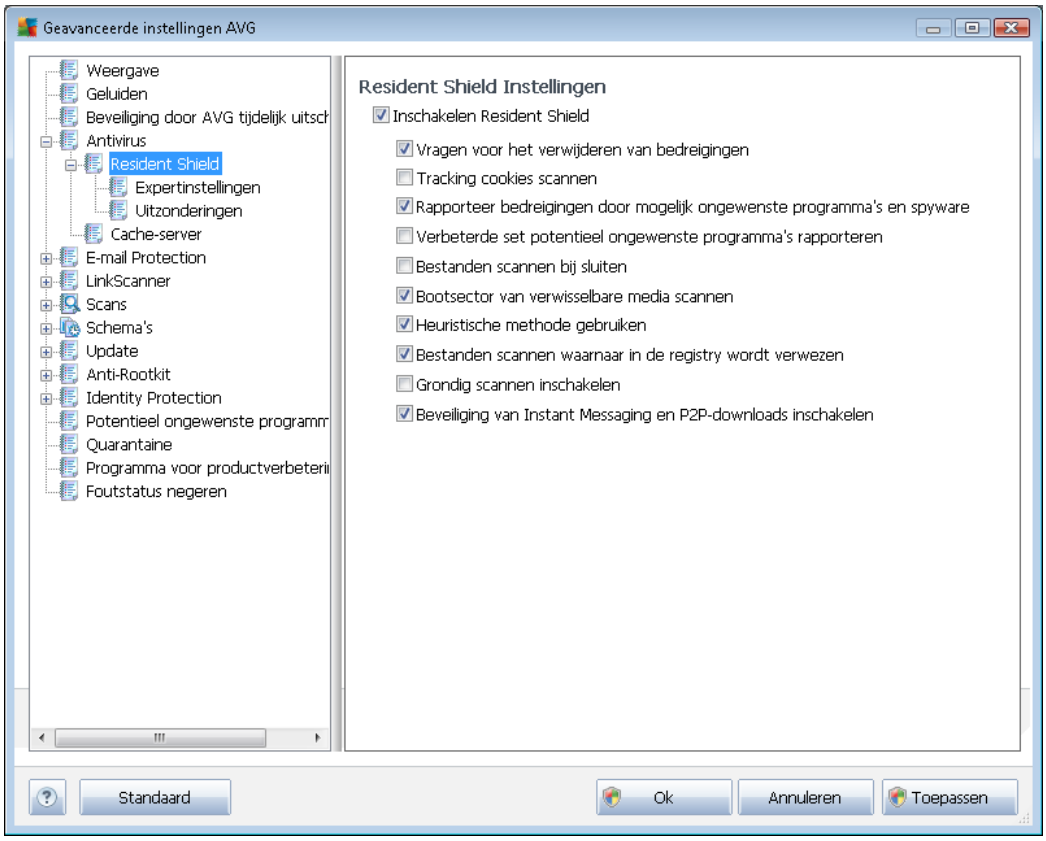
- Stel in het dialoogvenster ***Beveiliging door AVG tijdelijk uitschakelen*** dat wordt geopend in hoelang u **AVG Anti-Virus 2012** wilt uitschakelen. De beveiliging wordt gedurende 10 minuten uitgeschakeld. Dit is over het algemeen voldoende voor veelvoorkomende taken, zoals het installeren van nieuwe software, enzovoort. De standaardinstelling voor tijdsduur is maximaal 15 minuten. U kunt deze standaardperiode om veiligheidsredenen niet langer maken. Nadat de opgegeven periode is verstreken, worden alle gedeactiveerde onderdelen automatisch opnieuw geactiveerd.

9.4. Anti-Virus

Typ hier de tekst van het onderwerp.

9.4.1. Resident Shield

Resident Shield biedt live bescherming voor bestanden en mappen tegen virussen, spyware en andere malware.



U kunt in het dialoogvenster ***Resident Shield Instellingen*** de volledige residente beveiliging activeren of deactiveren door het selectievakje ***Resident Shield inschakelen*** in of uit te schakelen (*Deze optie is standaard ingeschakeld*). Daarnaast kunt u selecteren welke functies van de residente beveiliging u wilt activeren:

- ***Tracking cookies scannen*** (*is standaard uitgeschakeld*) - Deze parameter bepaalt dat cookies tijdens scannen moeten worden gedetecteerd. (*HTTP-cookies worden gebruikt voor verificatie, tracking en het bijhouden van bepaalde informatie over gebruikers, zoals voorkeuren voor websites of de inhoud van winkelwagentjes.*)

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

- ***Verbeterde set potentieel ongewenste programma's rapporteren*** (*is standaard uitgeschakeld*) - Schakel dit selectievakje in als u pakketten die met spyware zijn

uitgebreid, wilt detecteren. Dit zijn programma's die in orde en onschadelijk zijn wanneer u deze rechtstreeks van de fabrikant verkrijgt, maar die op een later tijdstip kunnen worden misbruikt voor schadelijke doeleinden. Dit is een aanvullende maatregel 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*** (*is standaard uitgeschakeld*) - Scannen bij het sluiten zorgt ervoor dat AVG actieve objecten (zoals toepassingen, documenten, enzovoort) scant wanneer deze worden geopend en wanneer deze worden gesloten. Deze functie beveiligt uw computer tegen bepaalde typen geavanceerde virussen.

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

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

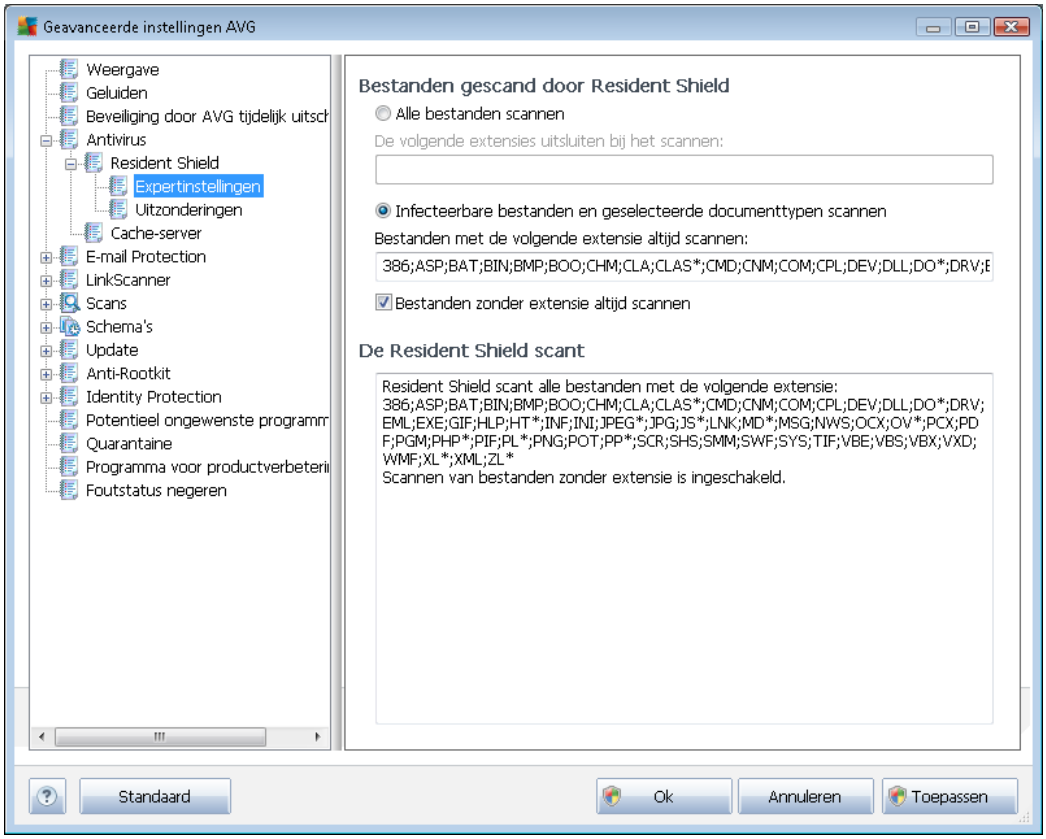
- ***Alle bedreigingen automatisch verwijderen*** (*is standaard uitgeschakeld*) – Eventueel gedetecteerde infecties worden automatisch hersteld als er een oplossing beschikbaar is. Alle infecties die niet kunnen worden hersteld, worden verwijderd.

- ***Bestanden scannen waarnaar in de registry wordt verwezen*** (*is standaard ingeschakeld*) – Deze parameter geeft aan dat AVG alle uitvoerbare bestanden scant die aan het opstartregister zijn toegevoegd, zodat wordt voorkomen dat een bekende infectie wordt uitgevoerd wanneer de computer de volgende keer opnieuw wordt opgestart.

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

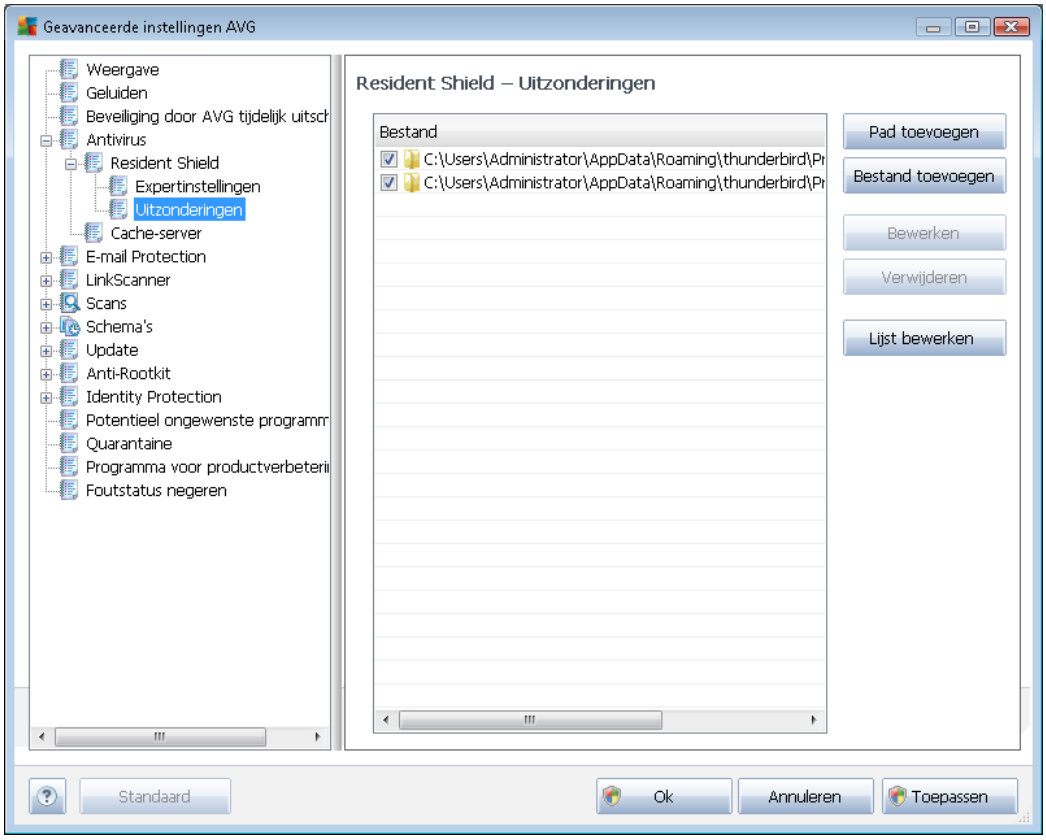
- ***Beveiliging van Instant Messaging en P2P-downloads inschakelen*** (*is standaard ingeschakeld*) - Schakel dit selectievakje in als u wilt controleren of communicatie via expresberichten (zoals via *ICQ, MSN Messenger, enzovoort.*) en P2P-downloads vrij zijn van virussen.

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



Schakel het desbetreffende selectievakje in om aan te geven of u de optie ***Alle bestanden scannen*** of alleen de optie ***Infecteerbare bestanden en geselecteerde documenttypen scannen*** wilt inschakelen. Als u de laatste optie kiest, kunt u vervolgens een lijst met extensies opgeven voor het definiëren van bestanden die moeten worden uitgesloten bij het scannen en u kunt een lijst met extensies opgeven voor het definiëren van bestanden die onder alle omstandigheden moeten worden gescand.

In het vak ***De Resident Shield scant***worden de huidige instellingen samengevat, samen met een uitgebreid overzicht van wat ***Resident Shield*** daadwerkelijk zal scannen.



In het dialoogvenster ***Resident Shield – Uitzonderingen*** kunt u mappen en bestanden opgeven die ***Resident Shield*** moet negeren bij het scannen.

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

Knoppen

Dit dialoogvenster heeft de volgende knoppen:

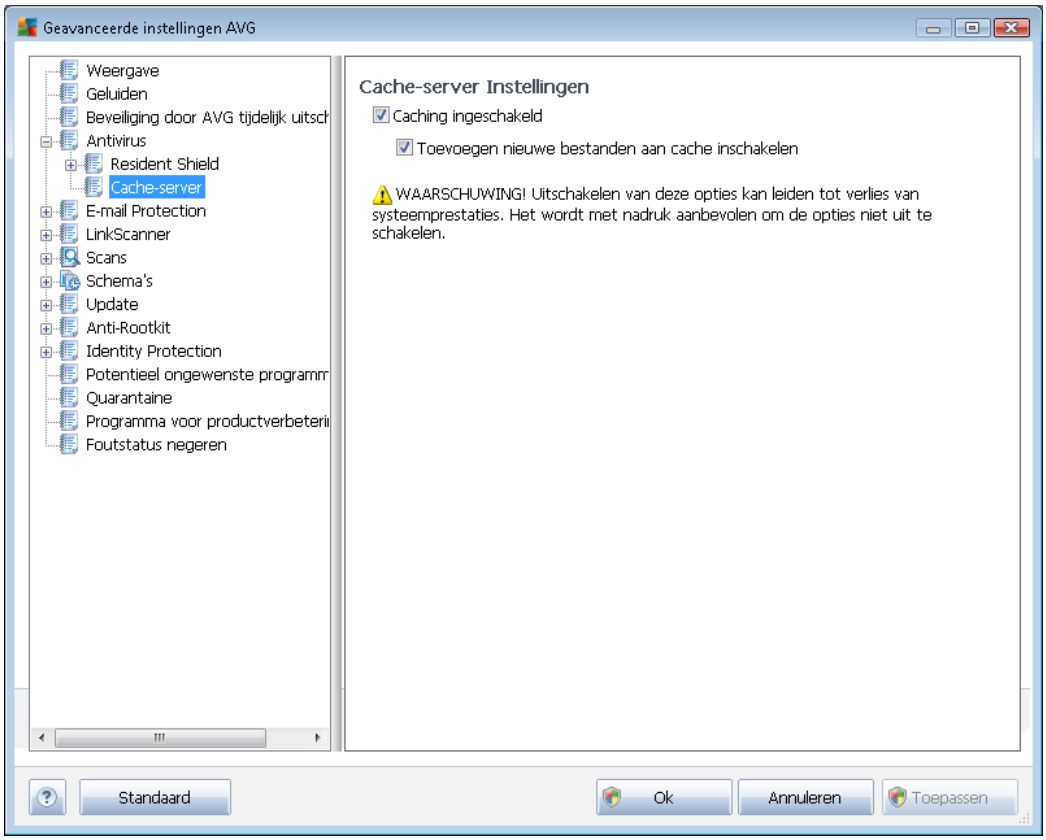
- ***Pad toevoegen*** – klik op deze knop om mappen op te geven die tijdens het scannen moeten worden overgeslagen. U kunt deze mappen vervolgens één voor één selecteren in de navigatiestructuur van de lokale schijf
- ***Bestand toevoegen*** – klik op deze knop om bestanden op te geven die tijdens het scannen moeten worden overgeslagen. U kunt deze bestanden vervolgens één voor één selecteren in de navigatiestructuur van de lokale schijf
- ***Item bewerken*** – klik op deze knop als u het opgegeven pad naar een geselecteerd bestand of een geselecteerde map wilt bewerken
- ***Verwijderen*** – klik op deze knop om het pad naar een geselecteerd item uit de lijst te

verwijderen

- ***Lijst bewerken*** – Klik op deze knop als u de gehele lijst met uitzonderingen wilt bewerken. Vervolgens wordt er een nieuw dialoogvenster weergegeven dat hetzelfde werkt als een standaardteksteditor

9.4.2. Cacheserver

Het dialoogvenster ***Instellingen Cache-server*** heeft betrekking op het cacheserverproces dat is ontworpen met het oog op het verhogen van de snelheid van alle typen **AVG Anti-Virus 2012**-scans:



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

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

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

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

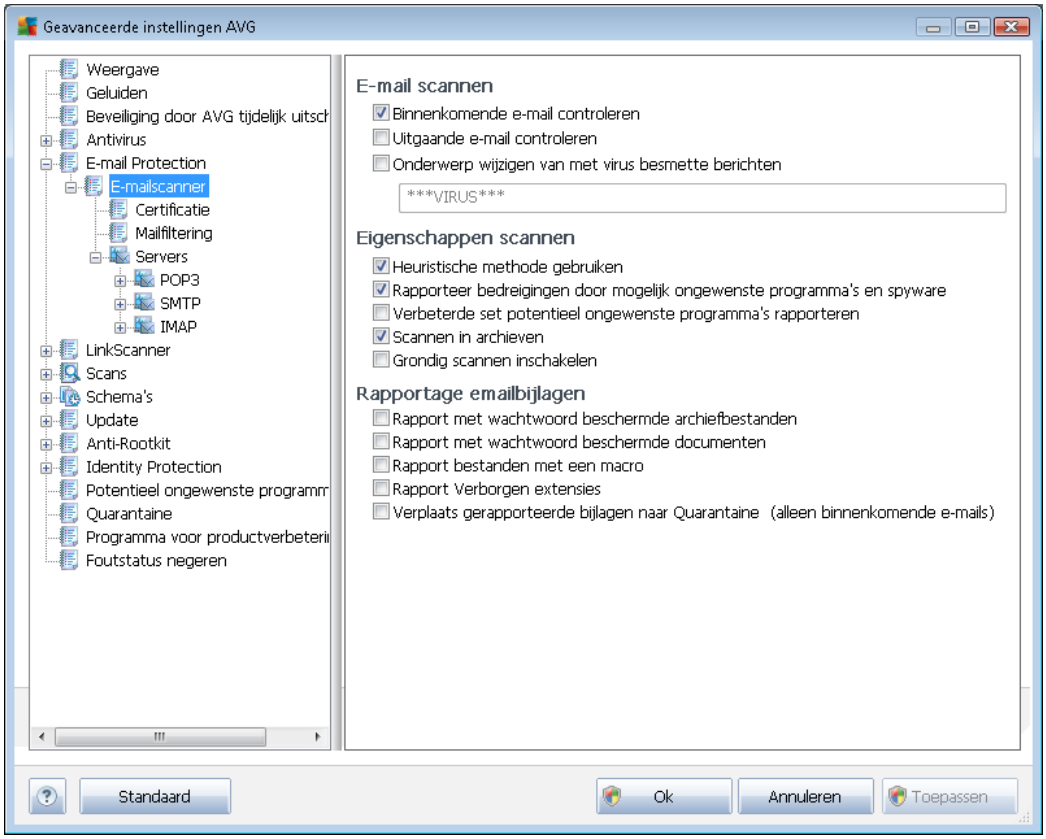
U wordt met klem aangeraden om de standaardinstellingen te behouden en beide opties ingeschakeld te laten, tenzij u over een goede reden beschikt om de cachteserver uit te schakelen. Als u dat niet doet, kan er een belangrijke achteruitgang van de snelheid en prestaties van uw systeem optreden.

9.5. E-mailbescherming

In de sectie ***E-mail Protection*** kunt u gedetailleerde configuratie-instellingen van de e-mailscanner en Anti-Spam bewerken:

9.5.1. E-mailscanner

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



E-mail scannen

E-mail scannen – in dit gedeelte kunt u het volgende instellen voor binnenkomende en uitgaande e-mailberichten:

- ***Binnenkomende e-mail scannen*** (*standaard ingeschakeld*) – Als het selectievakje wordt ingeschakeld, wordt alle bij uw e-mailclient binnenkomende e-mail gescand

- ***Uitgaande e-mail scannen*** (*standaard uitgeschakeld*) – Als het selectievakje wordt ingeschakeld, wordt alle door uw e-mailaccount verzonden e-mail gescand

- ***Onderwerp wijzigen van met virus geïnfecteerd bericht*** (*standaard uitgeschakeld*) – als u het selectievakje inschakelt, wordt u gewaarschuwd als er een geïnfecteerd bericht is gedetecteerd. 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 standaardwaarde is ***VIRUS***, het is raadzaam die te handhaven.

Scaneigenschappen

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

- ***Heuristische methode gebruiken*** (*standaard ingeschakeld*) – schakel dit selectievakje in om gebruik te maken van de heuristische detectiemethode voor het scannen van e-mailberichten. Als deze optie is ingeschakeld, kunt u e-mailbijlagen niet alleen op extensie filteren, maar wordt ook de feitelijke inhoud van de bijlage 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: ook al vormt het gewoonlijk een veiligheidsrisico, sommige van deze programma's worden met opzet geïnstalleerd. Het is raadzaam deze functie niet uit te schakelen, omdat hij de bescherming van uw computer vergroot.

- ***Verbeterde set potentieel ongewenste programma's rapporteren***(*standaard uitgeschakeld*) – schakel dit selectievakje in 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 archiefbestanden te scannen die aan e-mailberichten zijn gekoppeld als bijlage.*

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

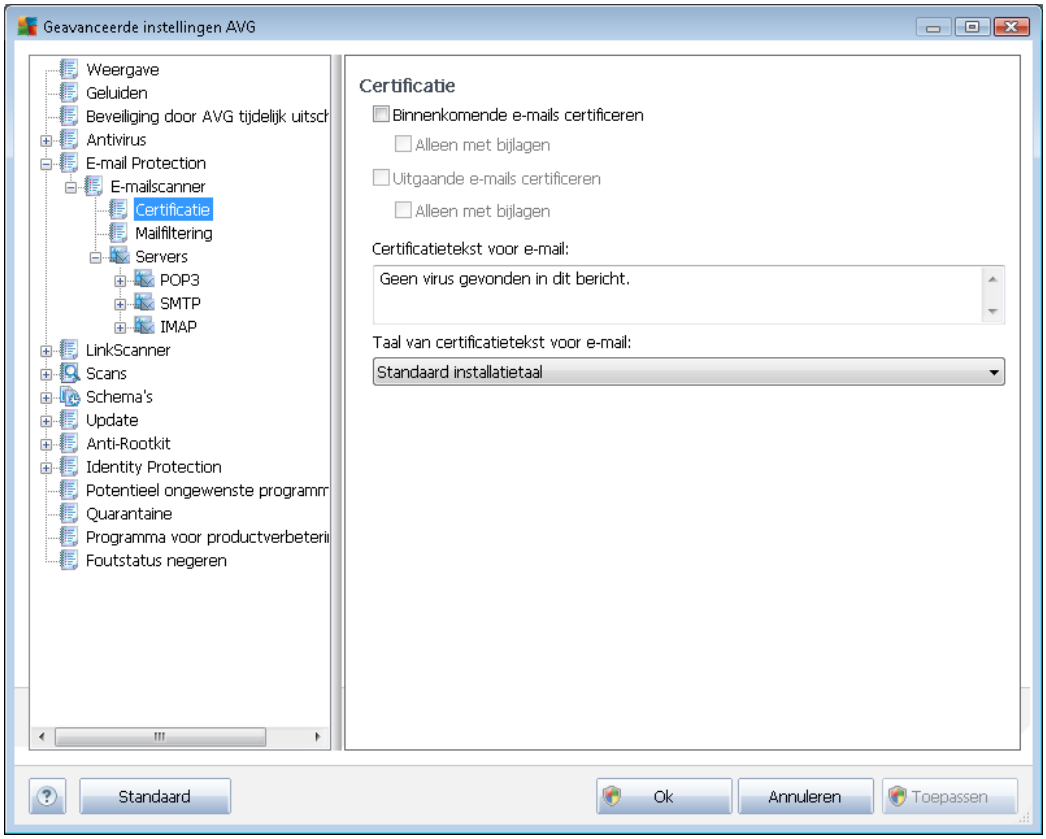
Rapportage e-mailbijlagen

In dit gedeelte kunt u extra rapportages instellen omtrent potentieel gevaarlijke of verdachte

bestanden. NB: er zal geen waarschuwingsvenster worden weergegeven, er wordt alleen een certificeringstekst toegevoegd aan het eind van het e-mailbericht en al dergelijke rapporten worden vermeld in het dialoogvenster E-mailscannerdetectie:

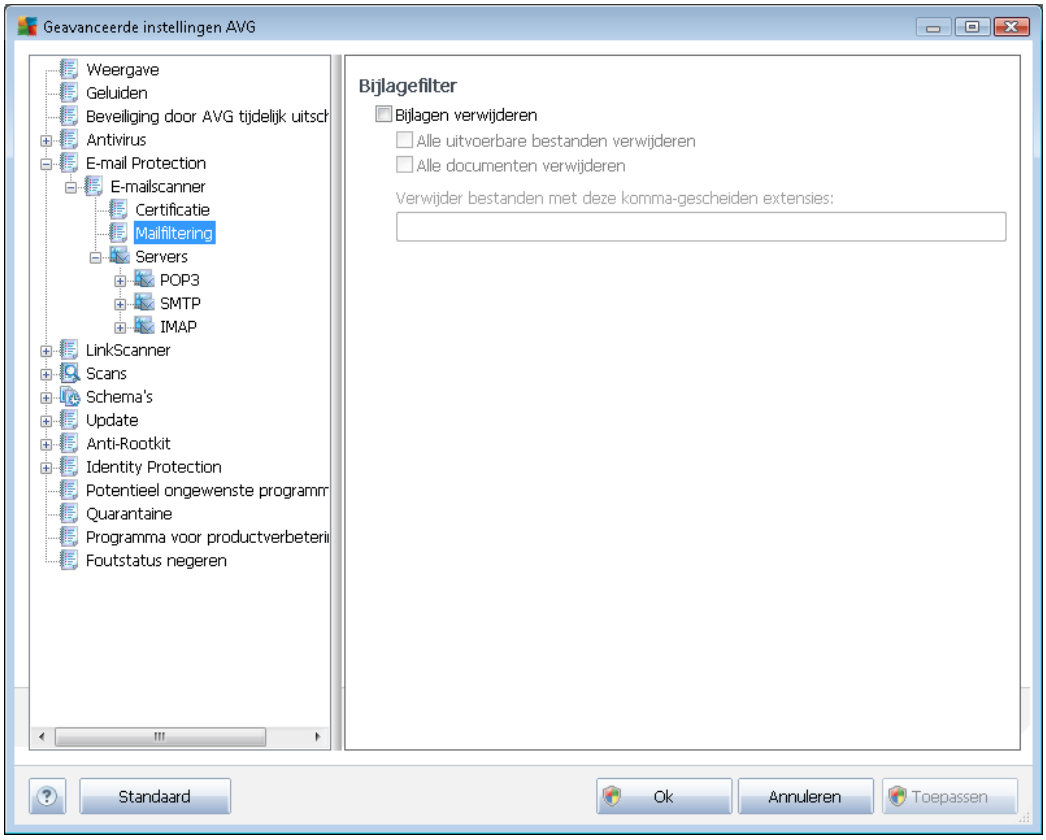
- ***Met een wachtwoord beveiligde archieven rapporteren*** – archieven (*zip, rar, enzovoort*)) die beveiligd zijn met een wachtwoord, kunnen niet op virussen worden gescand; schakel het selectievakje in om deze als potentieel gevaarlijk te rapporteren.
- ***Met een wachtwoord beveiligde documenten 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.
- ***Rapport bestanden met een macro*** – een macro is een vooraf gedefinieerd aantal stappen bedoeld om bepaalde taken voor een gebruiker te vergemakkelijken *(MS Word-macro's zijn alom bekend*). Daarom kan een macro potentieel gevaarlijke instructies bevatten; als u dit selectievakje inschakelt, worden bestanden met macro's als verdacht gerapporteerd.
- ***Rapport verborgen extensies*** – 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.

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



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

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



In het dialoogvenster ***Bijlagefilter*** kunt u parameters instellen voor het scannen van bijlagen bij e-mailberichten. Standaard is de optie ***Bijlagen verwijderen*** uitgeschakeld. Als u besluit die functie in te schakelen, worden 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:

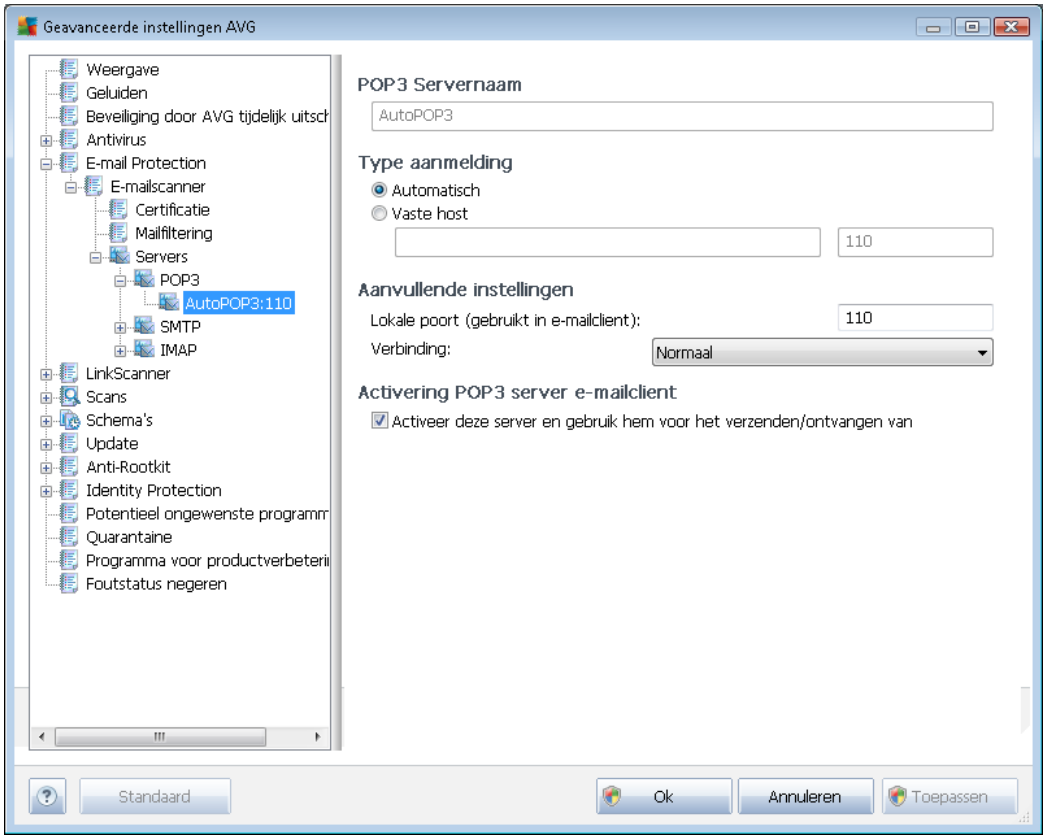
- ***Alle uitvoerbare bestanden verwijderen*** – alle bestanden met de extensie *.exe worden verwijderd
- ***Alle documenten verwijderen*** – alle bestanden met de extensie *.doc, *.docx, *.xls en *.xlsx worden verwijderd
- ***Bestanden met deze kommagescheiden extensies verwijderen*** – alle bestanden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

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

- POP3-server
- SMTP-server

- IMAP-server

Het is ook mogelijk om een nieuwe server voor binnenkomende en uitgaande e-mail in te stellen met de knop ***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*** – in dit veld kunt u de naam opgeven van nieuwe servers (*als u een POP3-server wilt opgeven, klikt u met de rechtermuisknop op het POP3-item in de navigatiestructuur links*). Bij een automatisch aangemaakte "AutoPOP3"-server wordt dit veld uitgeschakeld.

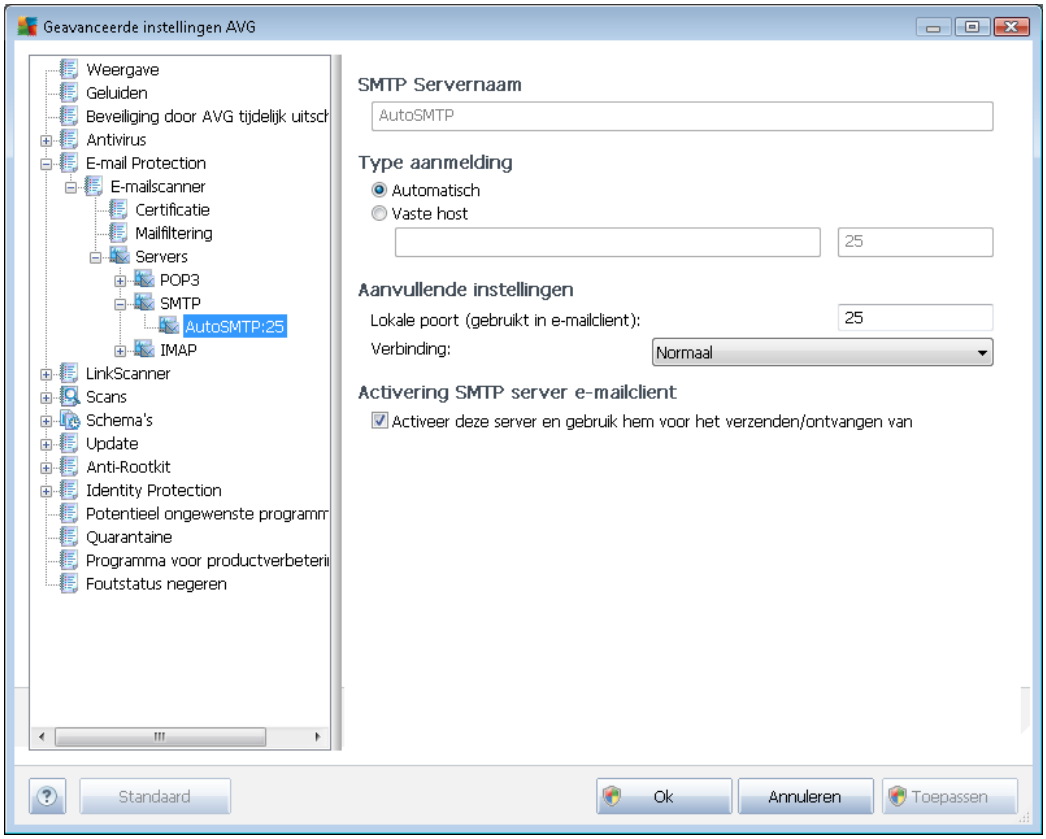
- ***Type aanmelding*** – bepalen van de methode voor het vaststellen van de mailserver die wordt gebruikt voor binnenkomende e-mailberichten:

  - ***Automatisch*** – Aanmelding wordt automatisch uitgevoerd, afhankelijk van de instellingen van uw e-mailclient.

  - ***Vaste host*** – In dit geval gebruikt het programma altijd de server die hier opgegeven is. Geef het adres of de naam van uw mailserver op. De aanmeldingsnaam blijft hetzelfde. U kunt een domeinnaam gebruiken (*bijvoorbeeld pop.acme.com*), evenals een IP-adres (*bijvoorbeeld 123.45.67.89*). Als de mailserver een niet-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.
  - ***Verbinding*** – met behulp van dit vervolgkeuzemenu kunt u opgeven welk type verbinding moet worden gebruikt (*Normaal/SSL/SSL-standaard*). Als u een SSL-verbinding kiest, worden de gegevens gecodeerd verzonden zonder dat ze door een derde partij gevolgd of gecontroleerd kunnen worden. Deze functie is ook alleen beschikbaar wanneer de doelmailserver de functie ondersteunt.
- ***Activering POP3 server e-mailclient*** – De opgegeven POP3-server in- of uitschakelen

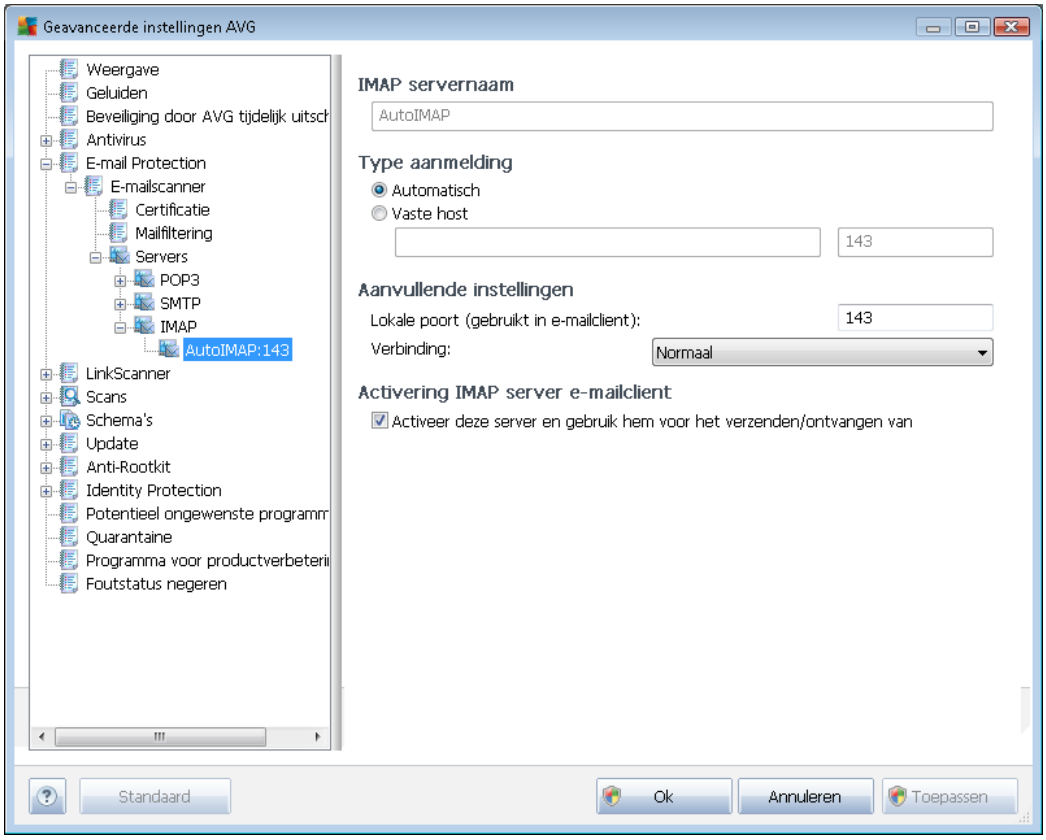


In dit dialoogvenster (*geopend met **Servers / SMTP***) kunt u een nieuwe server instellen voor E-mailscanner die gebruikmaakt van het SMTP-protocol voor uitgaande e-mail:

- ***SMTP-servernaam*** – in dit veld kunt u de naam opgeven van nieuwe servers (*als u een SMTP-server wilt opgeven, klikt u met de rechtermuisknop op het SMTP-item in de*

navigatiestructuur links). Bij een automatisch aangemaakte "AutoSMTP"-server wordt dit veld uitgeschakeld.

- ***Type aanmelding*** – bepalen van de methode voor het vaststellen van de mailserver die wordt gebruikt voor binnenkomende e-mailberichten:
    - ***Automatisch*** – aanmelding wordt automatisch uitgevoerd, met behulp van de instellingen voor uw e-mailclient
    - ***Vaste host*** – in dit geval gebruikt het programma altijd de server die hier opgegeven is. Geef het adres of de naam van uw mailserver op. U kunt een domeinnaam gebruiken (*bijvoorbeeld smtp.acme.com*), maar ook een IP-adres (*bijvoorbeeld 123.45.67.89*). Als de mailserver een niet-standaard poort gebruikt, kunt u deze poort na de servernaam opgeven. Gebruik een dubbele punt als scheidingsteken (*bijvoorbeeld smtp.acme.com:8200*). De standaardpoort voor SMTP-communicatie is 25.
- ***Aanvullende instellingen*** – 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.
    - ***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.
- ***E-mailclient SMTP-serveractivering*** – Schakel dit selectievakje in/uit om de genoemde SMTP-server te activeren/deactiveren



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

- ***IMAP-servernaam*** – in dit veld kunt u de naam opgeven van nieuwe servers (*als u een IMAP-server wilt opgeven, klikt u met de rechtermuisknop op het IMAP-item in de navigatiestructuur links*). Bij een automatisch aangemaakte "AutoIMAP"-server wordt dit veld uitgeschakeld.

- ***Type aanmelding*** – bepalen van de methode voor het vaststellen van de mailserver die wordt gebruikt voor binnenkomende e-mailberichten:

  - ***Automatisch*** – aanmelding wordt automatisch uitgevoerd, met behulp van de instellingen voor uw e-mailclient

  - ***Vaste host*** – in dit geval gebruikt het programma altijd de server die hier opgegeven is. Geef het adres of de naam van uw mailserver op. U kunt een domeinnaam gebruiken (*bijvoorbeeld smtp.acme.com*), maar ook een IP-adres (*bijvoorbeeld 123.45.67.89*). *Als de mailserver een niet-standaard poort gebruikt, kunt u deze poort na de servernaam opgeven. Gebruik een dubbele punt als scheidingsteken (bijvoorbeeld smtp.acme.com:8200*). De standaardpoort voor IMAP-communicatie is 143.

- ***Aanvullende instellingen*** – 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.

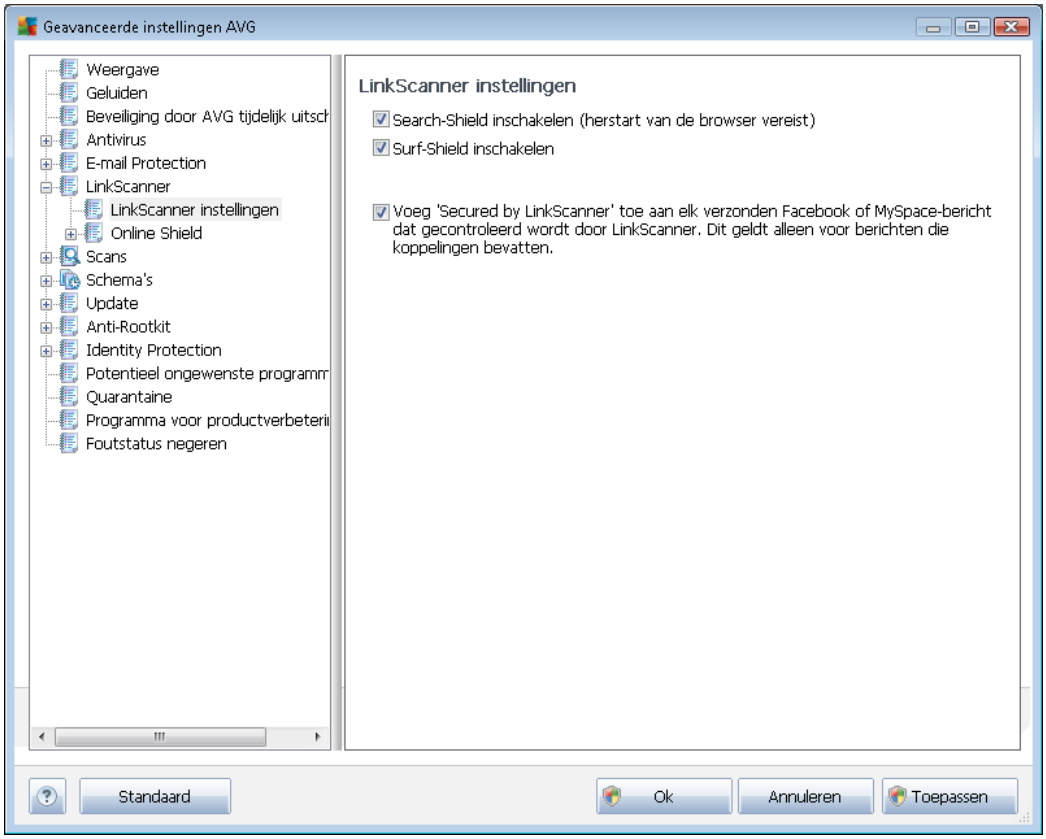
- ***Verbinding*** – *met behulp van dit vervolgkeuzemenu kunt u opgeven welk type verbinding moet worden gebruikt (Normaal/SSL/SSL-standaard).* Als u een SSL-verbinding kiest, worden de gegevens gecodeerd verzonden zonder dat ze door een derde partij gevolgd of gecontroleerd kunnen worden. Deze functie is alleen beschikbaar wanneer de doelmailserver de functie ondersteunt.

- ***E-mailclient IMAP-serveractivering*** – Schakel dit selectievakje in/uit om de genoemde IMAP-server te activeren/deactiveren

9.6. LinkScanner

9.6.1. Instellingen LinkScanner

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



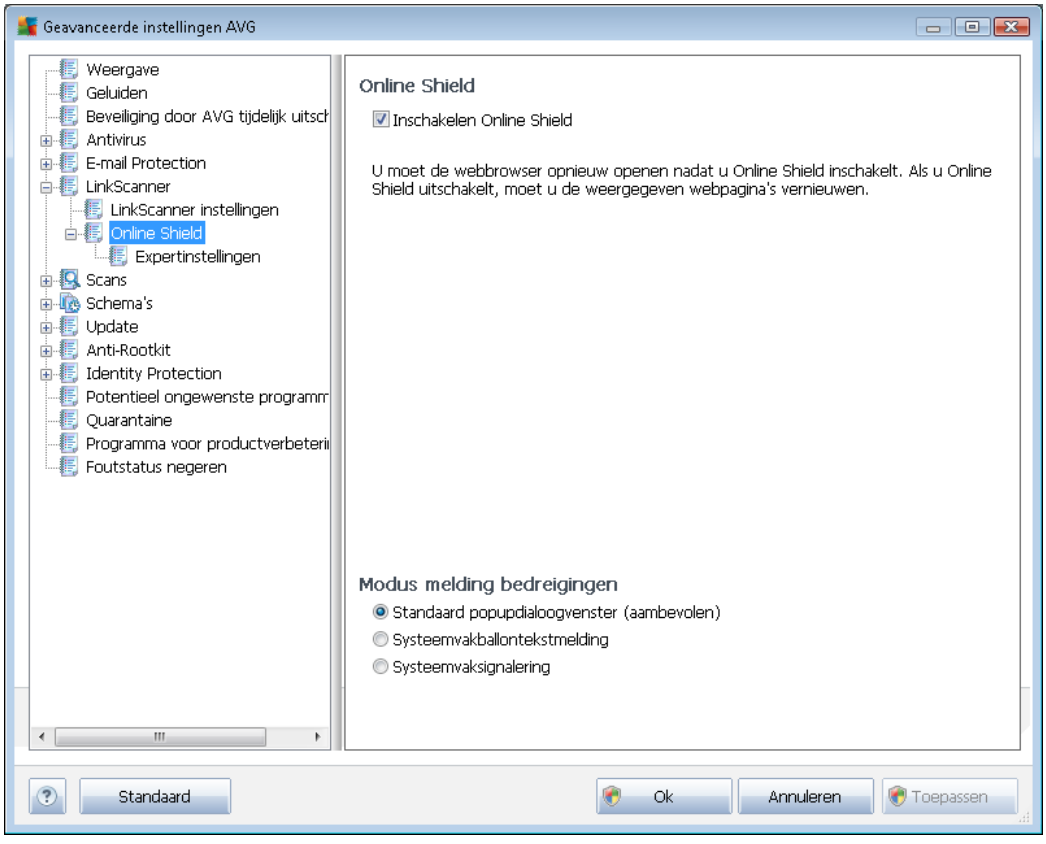
- Search-Shield *inschakelen* – *(*standaard ingeschakeld) pictogrammen die een oordeel geven over de resultaten met zoekmachines van Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg en SlashDot: de

gegevens van de zoekmachine worden eerst gecontroleerd.

- ***Surf-Shield inschakelen*** (*standaard ingeschakeld*) – actieve (*realtime*) 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*).

- ***Voeg 'Beveiligd met LinkScanner' toe...*** – (*standaard ingeschakeld*): markeer dit item om te bevestigen dat u de certificatiemelding over LinkScanner wilt toevoegen voor het controleren van alle berichten met actieve hyperlinks, die zijn verzonden vanaf de sociale netwerken Facebook en MySpace.

9.6.2. Online Shield



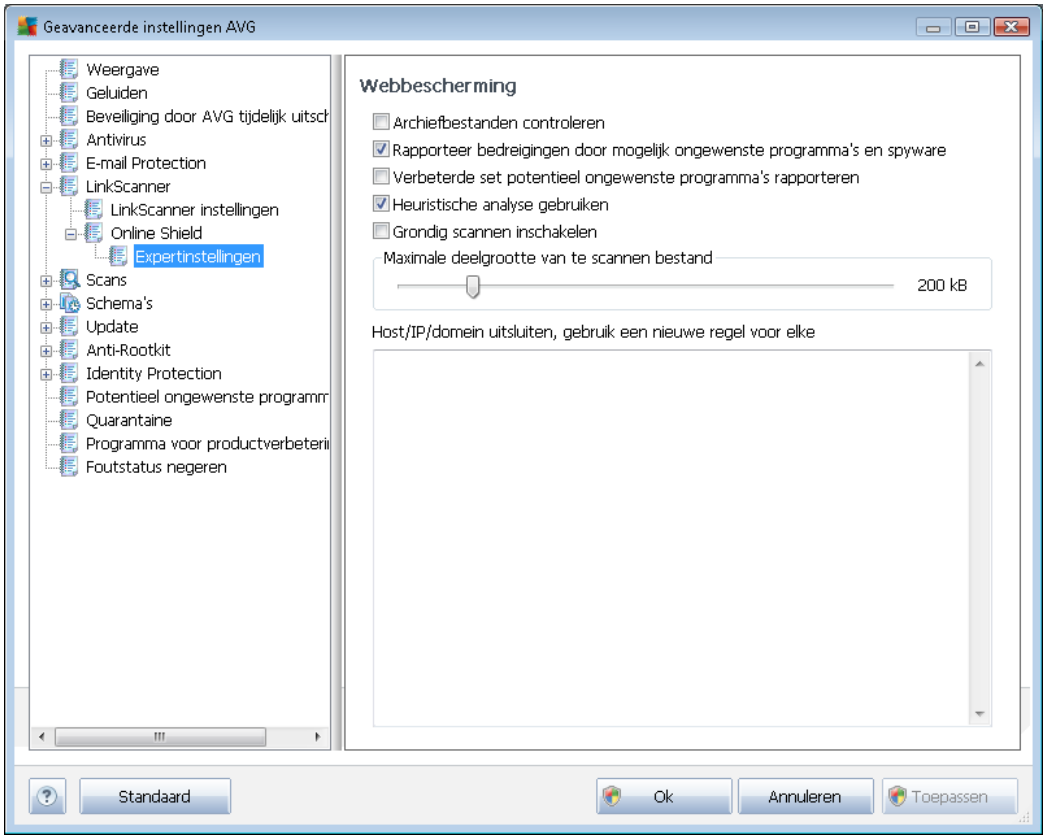
Het dialoogvenster ***Online Shield*** bevat de volgende opties:

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

- ***AVG accelerator inschakelen*** *(standaard ingeschakeld)* – hiermee kunt u de ***AVG Accelerator***-service inschakelen en uitschakelen. Deze service biedt soepeler afspelen van online video en vereenvoudigt aanvullende downloads.

Modus melding bedreigingen

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



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

- ***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 (als *standaard*), kunt u nog de volgende functies in- en uitschakelen:
    - ***Archiefbestanden controleren***(*standaard uitgeschakeld*) – de inhoud van archieven scannen die zijn ingesloten op de webpagina's die u wilt weergeven.
    - ***Potentieel ongewenste programma's en spywarebedreigingen rapporteren*** – (*standaard ingeschakeld*): schakel dit selectievakje in om het Anti-Spyware-programma te activeren, zodat er naast op virussen ook op spyware wordt gescand. Spyware behoort tot een twijfelachtige categorie malware: ook al vormt het gewoonlijk een veiligheidsrisico, sommige van deze programma's worden met opzet

geïnstalleerd. Het is raadzaam deze functie niet uit te schakelen, omdat hij de bescherming van uw computer vergroot.

- ***Uitgebreide sets van mogelijk ongewenste programma's rapporteren*** (*standaard uitgeschakeld*) – schakel dit selectievakje in 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*** (*standaard ingeschakeld*) – de inhoud scannen van een weer te geven pagina met behulp van de methode voor heuristische analyse (*dynamische emulatie van de instructies van gescande objecten in een virtuele computeromgeving*).

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

- ***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.

9.7. Scans

De geavanceerde scaninstellingen zijn onderverdeeld in vier 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

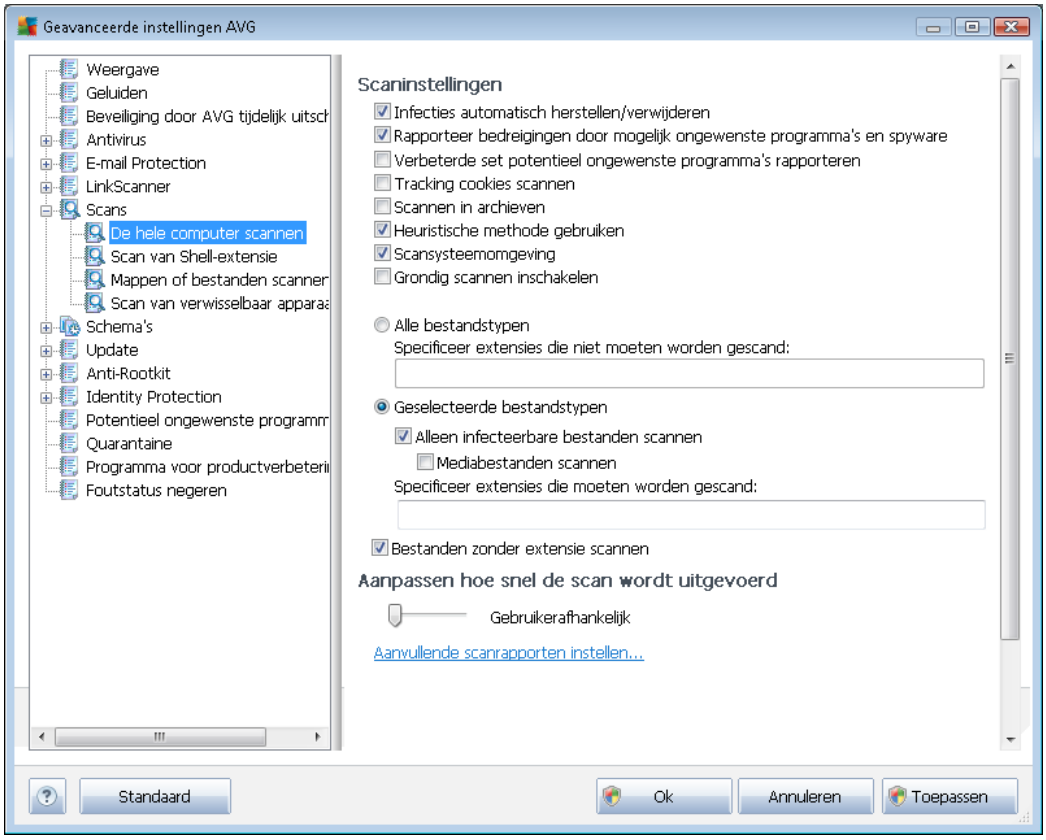
- ***Shell-extensie scannen*** – scannen van een specifiek object direct in de Windows Verkenner

- ***Bepaalde mappen of bestanden scannen*** – een 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

9.7.1. De hele computer scannen

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



Scaninstellingen

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

- ***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 kan worden hersteld, wordt het naar de map Quarantaine verplaatst.

- ***Bedreigingen door mogelijk ongewenste programma's en spyware rapporteren*** (*standaard ingeschakeld*) – schakel dit selectievakje in om het Anti-Spyware-programma te activeren en op spyware en virussen te scannen. Spyware behoort tot een twijfelachtige categorie malware: ook al vormt het gewoonlijk een veiligheidsrisico, sommige van deze programma's worden met opzet geïnstalleerd. Het is raadzaam deze functie niet uit te

schakelen, omdat hij de bescherming van uw computer vergroot.

- ***Verbeterde set potentieel ongewenste programma's rapporteren*** (*standaard uitgeschakeld*) – schakel dit selectievakje in als u pakketten die met spyware zijn uitgebreid, wilt detecteren. Dit zijn programma's die in orde en onschadelijk zijn wanneer u deze rechtstreeks van de fabrikant verkrijgt, maar die op een later tijdstip kunnen worden misbruikt voor schadelijke doeleinden. Dit is een aanvullende maatregel 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 uitgeschakeld*) – 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*** (*standaard uitgeschakeld* – met deze parameter bepaalt u of alle bestanden moeten worden gescand, ook die bestanden die zijn gecomprimeerd in archiefbestanden, bijv. ZIP, RAR, enz.

- ***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.

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

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.

Scansnelheid aanpassen

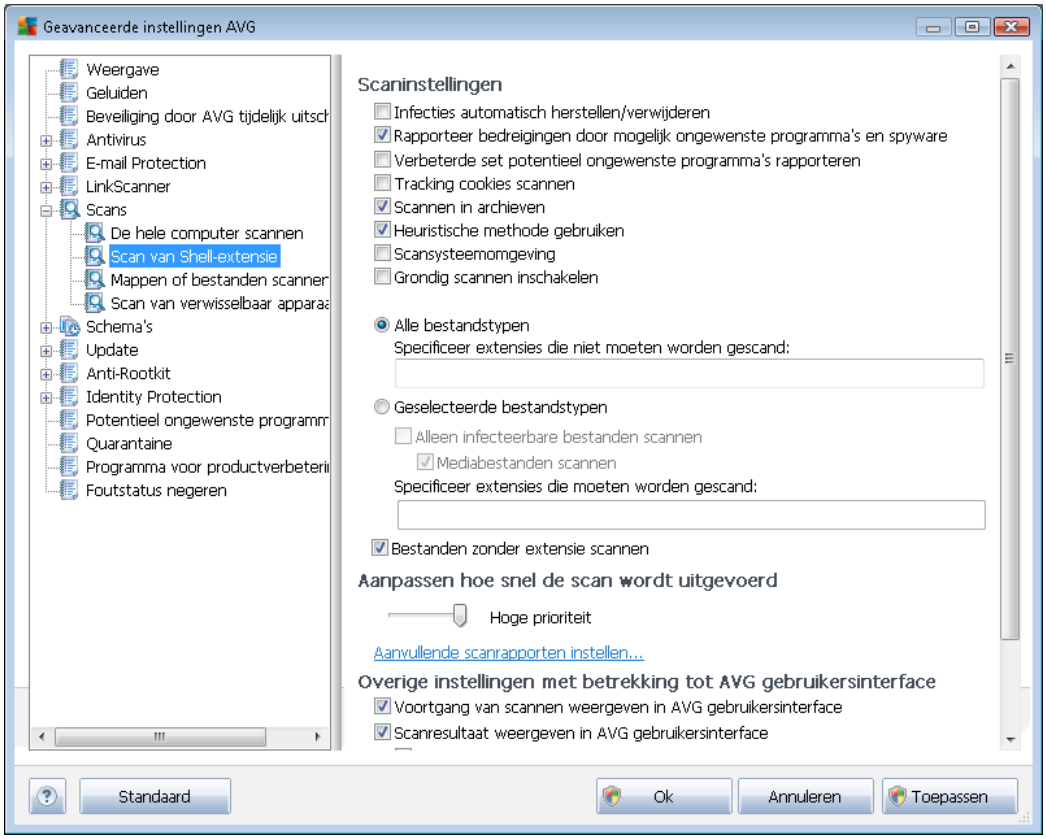
In het gedeelte ***Scansnelheid aanpassen*** kunt u nader specificeren hoe snel moet worden gescand in samenhang met het beroep dat wordt gedaan op de systeembronnen. Standaard is deze functie ingesteld op het niveau *gebruikerafhankelijk* voor gebruik van systeembronnen. Als u sneller wilt scannen, 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.

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:

9.7.2. Scan van Shell-extensie

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



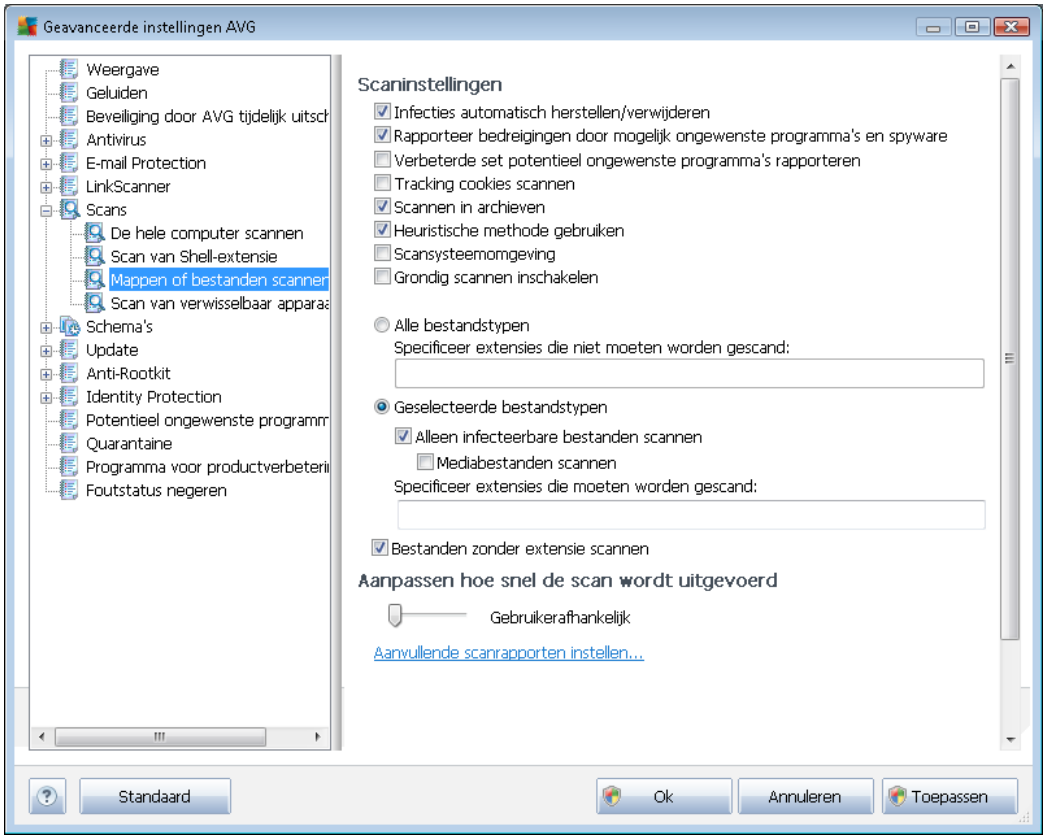
De lijst met beschikbare parameters is dezelfde als die van De hele computer scannen. De standaardinstellingen verschillen echter (*bij het scannen van de hele computer worden bijvoorbeeld archiefbestanden overgeslagen, maar wordt de systeemomgeving wel gescand, terwijl het bij de Shell-extensiescan net andersom is*).

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

Vergeleken met het dialoogvenster De hele computer scannen heeft het dialoogvenster ***Scan van Shell-extensie*** een extra sectie met de naam ***Overige instellingen met betrekking tot de AVG-gebruikersinterface***, waarin u kunt opgeven of de scanvoortgang en de scanresultaten ook bereikbaar moeten zijn vanuit de gebruikersinterface van AVG. Bovendien kunt u opgeven dat het scanresultaat alleen moet worden weergegeven als er tijdens het scannen een infectie is gedetecteerd.

9.7.3. 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:

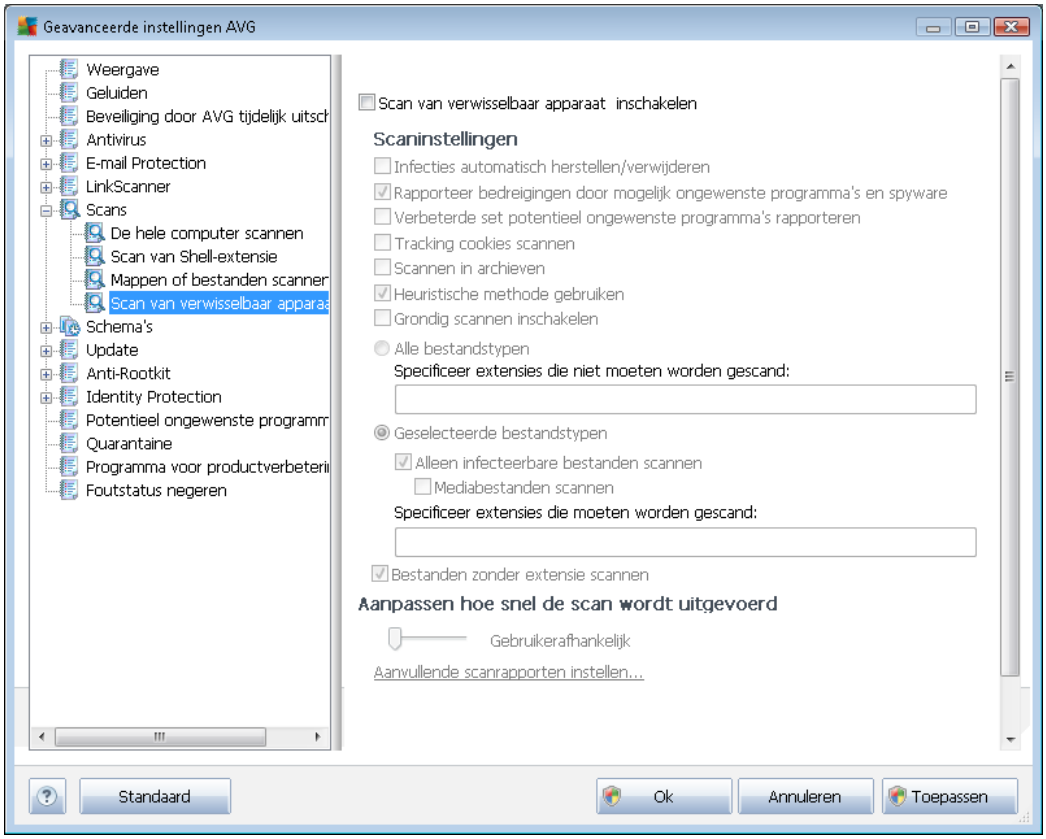


Alle parameters die u instelt in dit configuratiedialoogvenster hebben alleen betrekking op het scannen met de optie Bepaalde mappen of bestanden scannen!

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

9.7.4. 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 apparaat op de computer aansluit. Standaard is deze scanfunctie uitgeschakeld. Het is echter van essentieel belang om verwisselbare apparaten te scannen op potentiële bedreigingen omdat ze een belangrijke bron van infecties zijn. Om 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.*

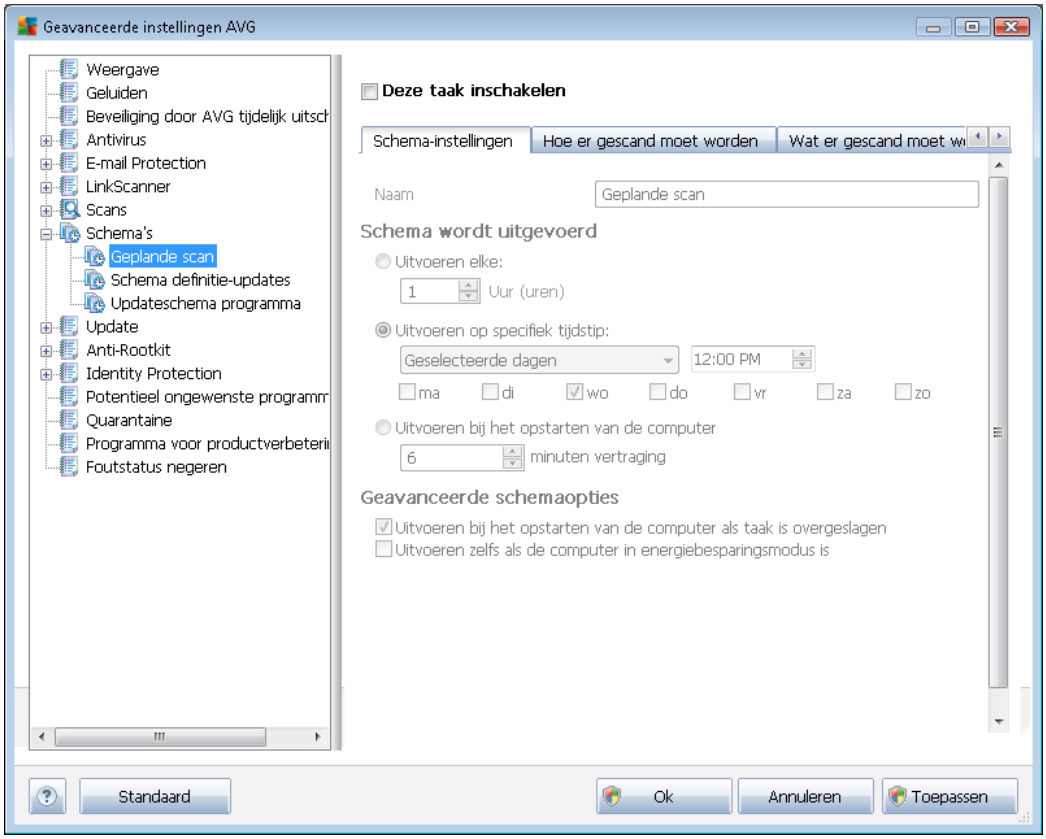
9.8. Schema's

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

- Geplande scan
- Schema definitie-updates
- Updateschema programma

9.8.1. Geplande scan

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



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.*

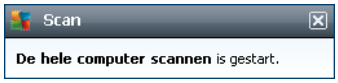
In dit dialoogvenster kunt u daarnaast nog de volgende parameters instellen:

Schema wordt uitgevoerd

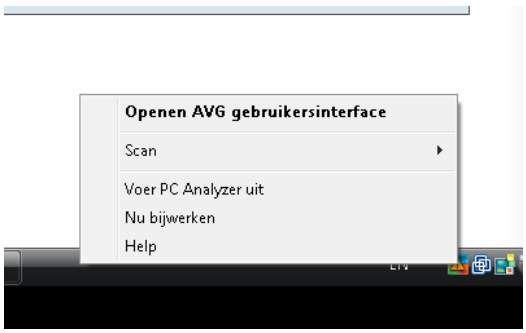
Hier kunt u tijdsintervallen opgeven waarmee de nieuwe geplande scan moet worden uitgevoerd. U kunt dit interval op verschillende manieren definiëren: als herhaalde scan die na verloop van een bepaalde tijd (***Uitvoeren elke .....***) moet worden uitgevoerd, als een scan die op een bepaalde datum op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

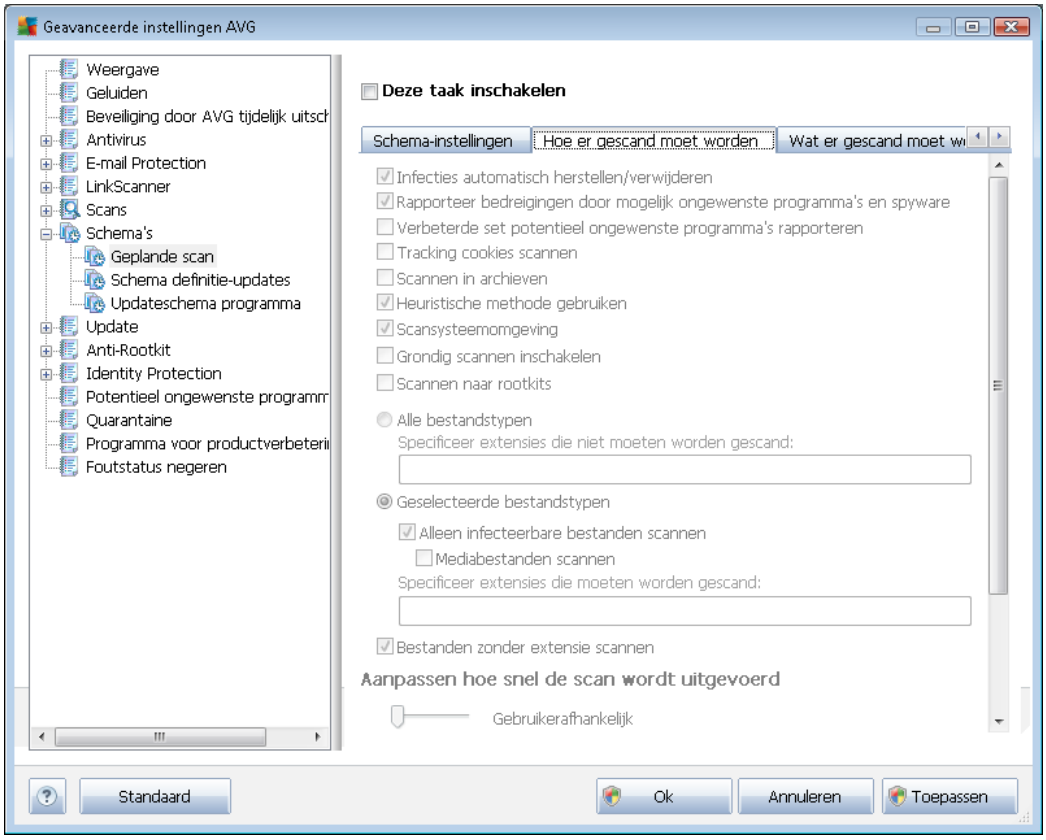
Geavanceerde schemaopties

In deze sectie kunt u bepalen onder welke omstandigheden de scan wel of niet moet worden uitgevoerd als de computer zich in een energiebesparingsmodus bevindt of als deze 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 bij het systeemvakpictogram van AVG:



Vervolgens verschijnt er een nieuw systeemvakpictogram van AVG (*in kleur met een flitslicht – 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 snelmenu te openen waarin u opties kunt kiezen om de scan te onderbreken of af te breken, of de prioriteit te wijzigen van de scan die wordt uitgevoerd:





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 (****standaard ingeschakeld*) – als tijdens het scannen een virus wordt gedetecteerd, wordt automatisch een herstelprocedure gestart, als die beschikbaar is. Als het geïnfecteerde bestand niet automatisch kan worden hersteld, wordt het naar de 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: ook al vormt het gewoonlijk een veiligheidsrisico, sommige van deze programma's worden met opzet geïnstalleerd. Het is raadzaam deze functie niet uit te schakelen, omdat hij de bescherming van uw computer vergroot.

- ***Verbeterde set potentieel ongewenste programma's rapporteren*** (*standaard uitgeschakeld*) – schakel dit selectievakje in 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;

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

- ***Scannen naar rootkits*** (*standaard uitgeschakeld*) – 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.

Scansnelheid aanpassen

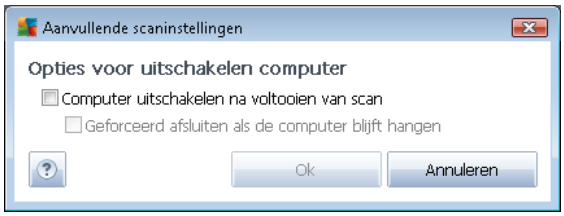
In het gedeelte ***Scansnelheid aanpassen*** kunt u nader specificeren hoe snel moet worden gescand in samenhang met het beroep dat wordt gedaan op de systeembronnen. Standaard is deze functie ingesteld op het niveau *gebruikerafhankelijk* voor gebruik van systeembronnen. Als u sneller wilt scannen, 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 systeembronnen ook verkleinen door te kiezen voor een langere scanduur.

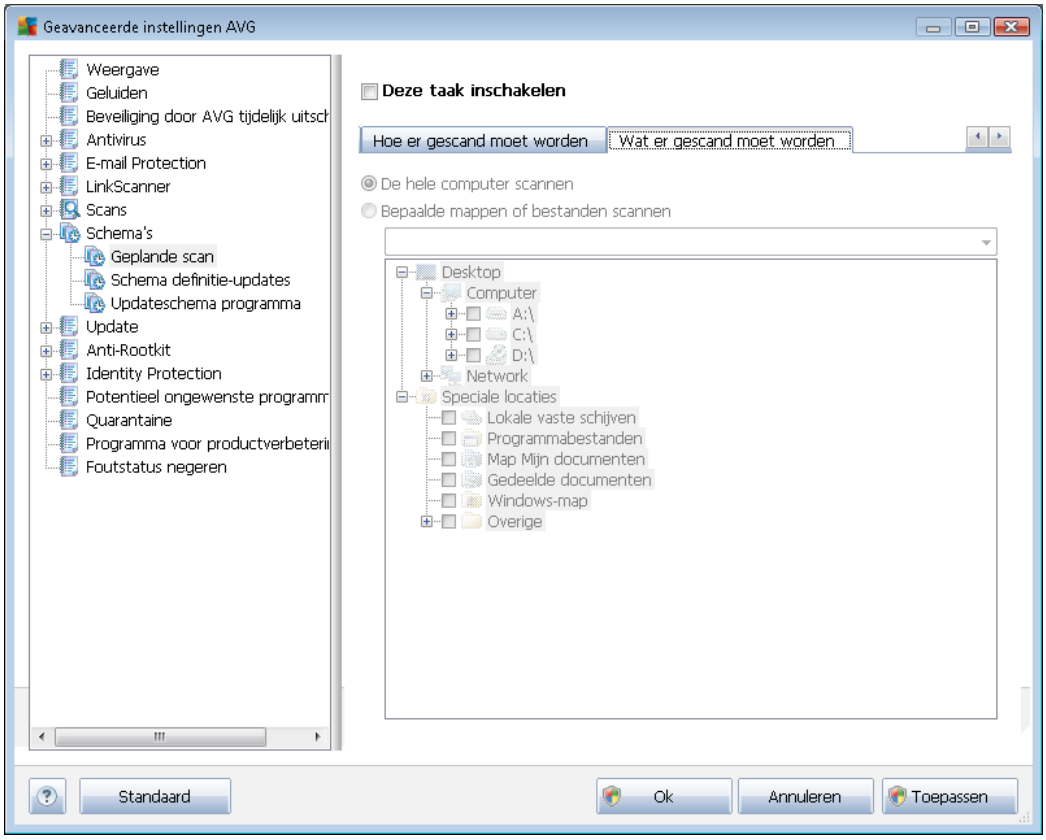
Aanvullende scanrapporten instellen

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:

Aanvullende scaninstellingen

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***).

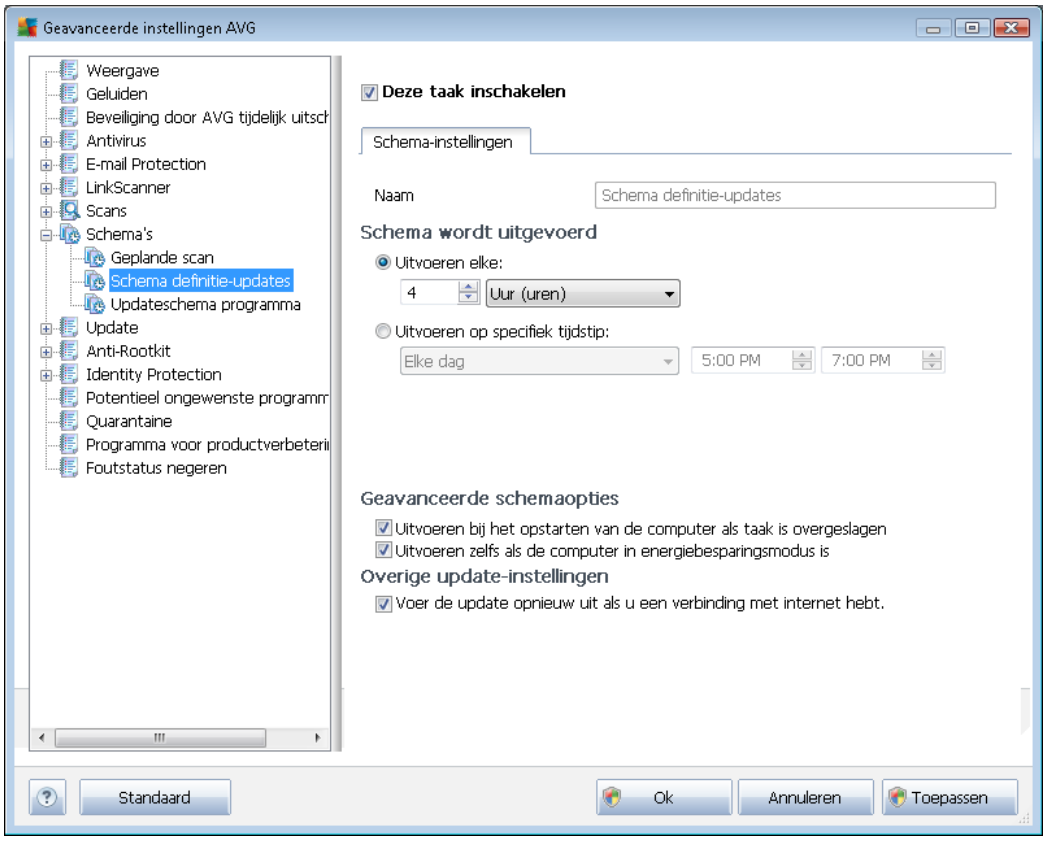




Op het tabblad ***Wat er gescand moet worden*** kunt u opgeven welke scan moet worden uitgevoerd: een scan van de hele computer of een scan van specifieke bestanden of mappen. Als u kiest voor het scannen van specifieke bestanden of mappen, wordt de in het onderste deel van het dialoogvenster weergegeven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

9.8.2. Schema voor definitie-updates

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



In dit dialoogvenster kunt u gedetailleerde instellingen opgeven voor het updateschema van de definities. In het vak ***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 die moeten worden gehanteerd voor het starten van de nieuwe geplande definitie-update. U kunt dat interval op verschillende manieren definiëren: als steeds terugkerende update die na verloop van een bepaalde tijd (***Uitvoeren elke ...***) moet worden uitgevoerd, of als update die op een bepaalde datum en een bepaald tijdstip (***Uitvoeren op specifiek tijdstip ...***) moet worden uitgevoerd.

Geavanceerde schemaopties

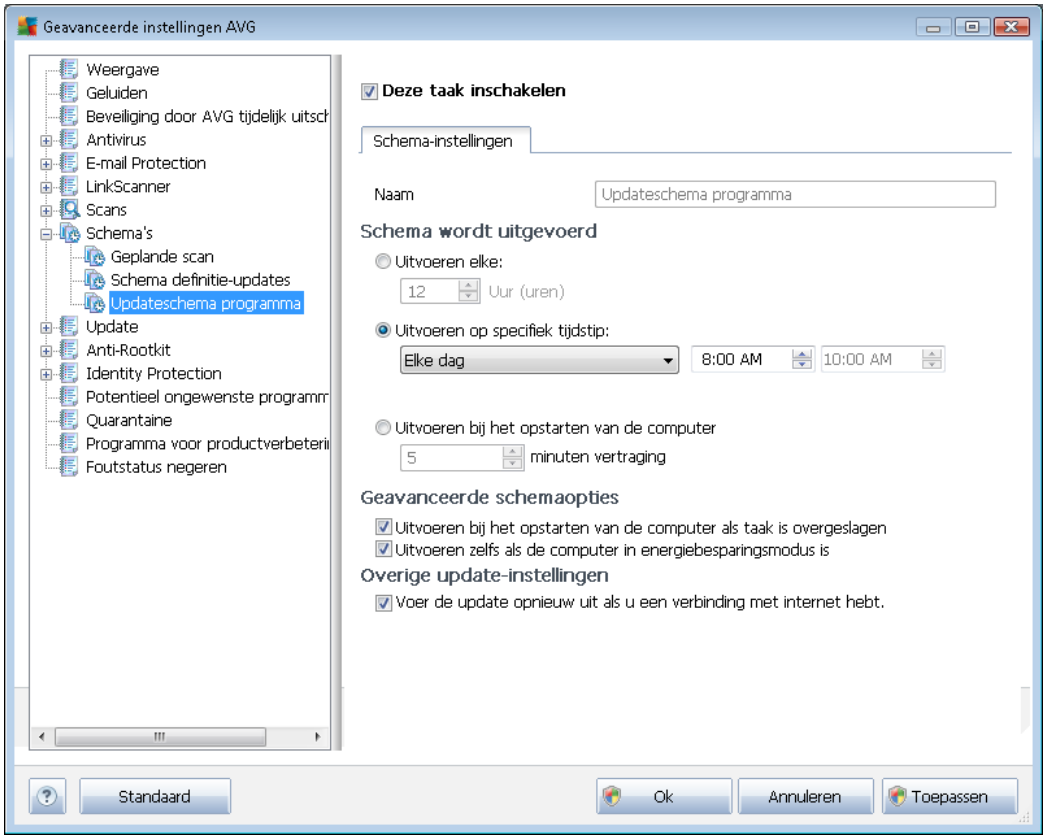
In deze sectie kunt u instellen onder welke omstandigheden de definitie-update wel of niet moet worden uitgevoerd als de computer zich in een energiebesparingsmodus bevindt of is uitgeschakeld.

Overige update-instellingen

Schakel tot slot het selectievakje in bij ***Voer de update opnieuw uit als u een verbinding met internet hebt*** om ervoor te zorgen dat, als de internetverbinding verbroken wordt en de updateprocedure mislukt, deze 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 bij het AVG-systeemvakpictogram (*als u de standaardconfiguratie van het dialoogvenster Geavanceerde instellingen/Weergave niet hebt gewijzigd).*

9.8.3. Updateschema programma

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



In het vak ***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.

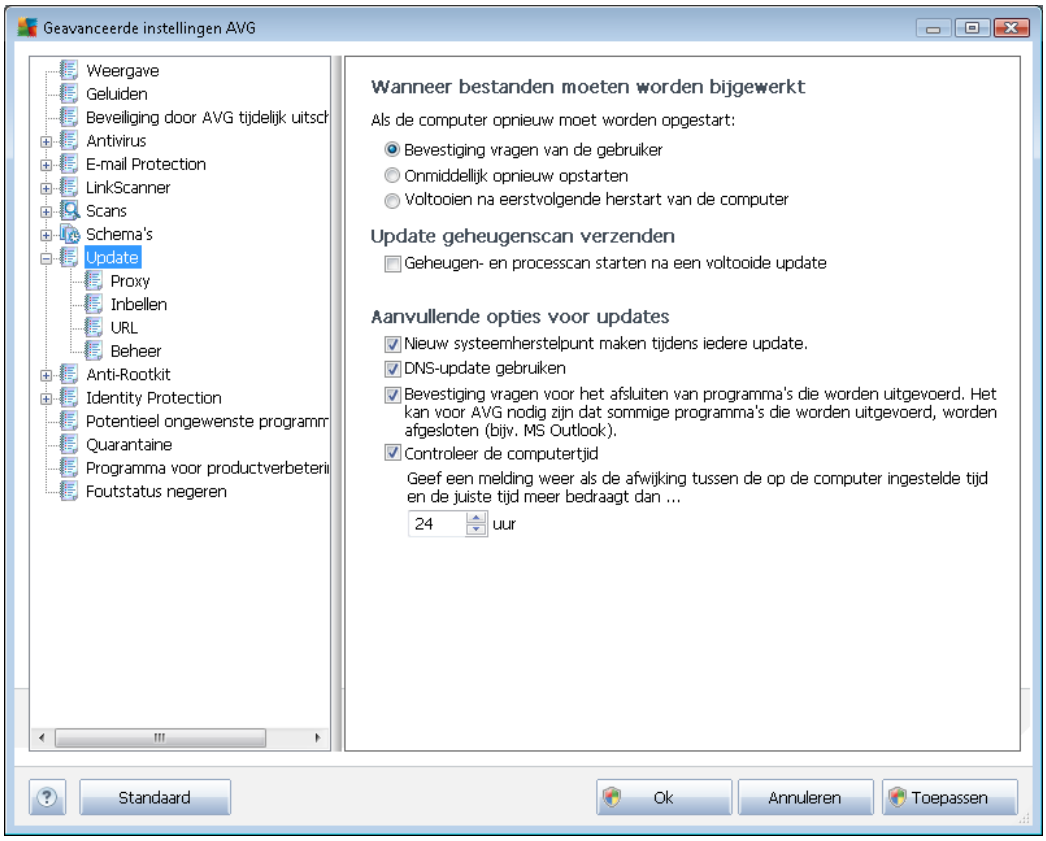
Overige update-instellingen

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.*

9.9. 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 dit gedeelte kunt u een keuze maken uit drie alternatieven als het updateproces een herstart van de computer vereist Het voltooien van de update kan worden gepland voor de eerstvolgende start van de computer, maar u kunt de herstart ook meteen uitvoeren:

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

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

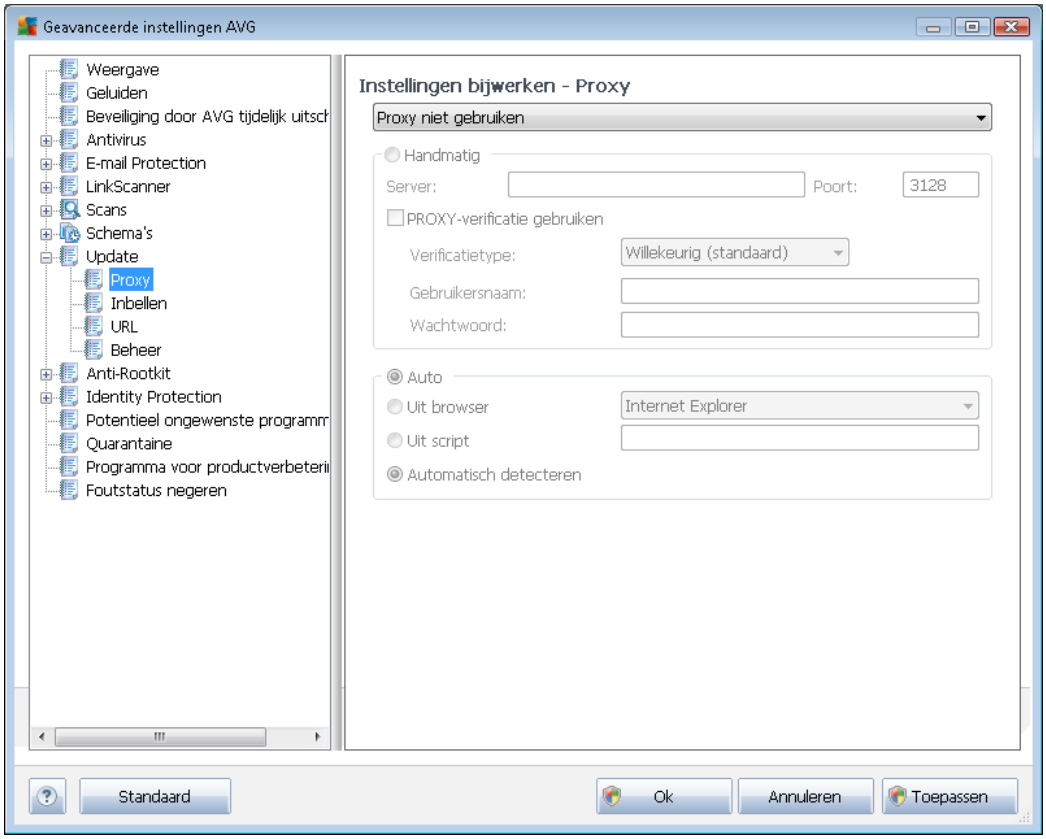
- ***Nieuw systeemherstelpunt maken na iedere programma-update*** – er wordt een nieuw systeemherstelpunt gemaakt voor elke programma-update van AVG. Als de updateprocedure faalt en uw besturingssysteem crasht, kunt u uw besturingssysteem altijd herstellen in de oorspronkelijke configuratie vanaf dit 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*** (*standaard ingeschakeld*) – als de update eenmaal is gestart, wordt door **AVG Anti-Virus 2012** op de DNS-server gezocht naar informatie over de nieuwste versies van de virusdatabase en het programma. Vervolgens worden alleen de kleinste, onmisbare bestanden gedownload en geïmplementeerd. Dat reduceert het totaal aan gedownloade gegevens tot een minimum en maakt de update sneller.

- ***Bevestiging vragen voor het afsluiten van programma's die worden uitgevoerd*** (*standaard ingeschakeld*) – deze optie zorgt ervoor dat toepassingen die worden uitgevoerd niet zullen worden gesloten zonder uw nadrukkelijke toestemming, indien dat nodig zou zijn voor het voltooien van de updateprocedure.

- ***Controleer de computertijd*** – schakel dit selectievakje in als er een melding moet worden weergegeven wanneer de computertijd met meer dan een opgegeven aantal uren afwijkt van de juiste tijd.

9.9.1. 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***
- ***Proxy niet gebruiken*** – standaardinstellingen
- ***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.

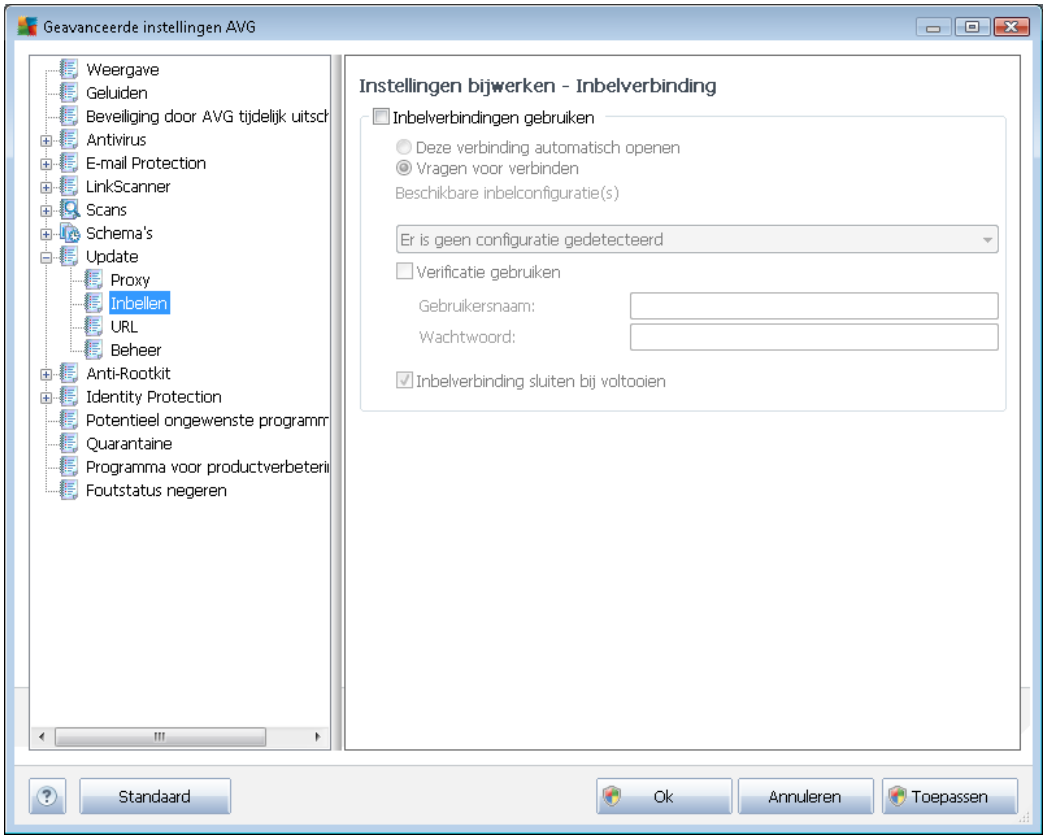
Automatische configuratie

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

9.9.2. Inbellen

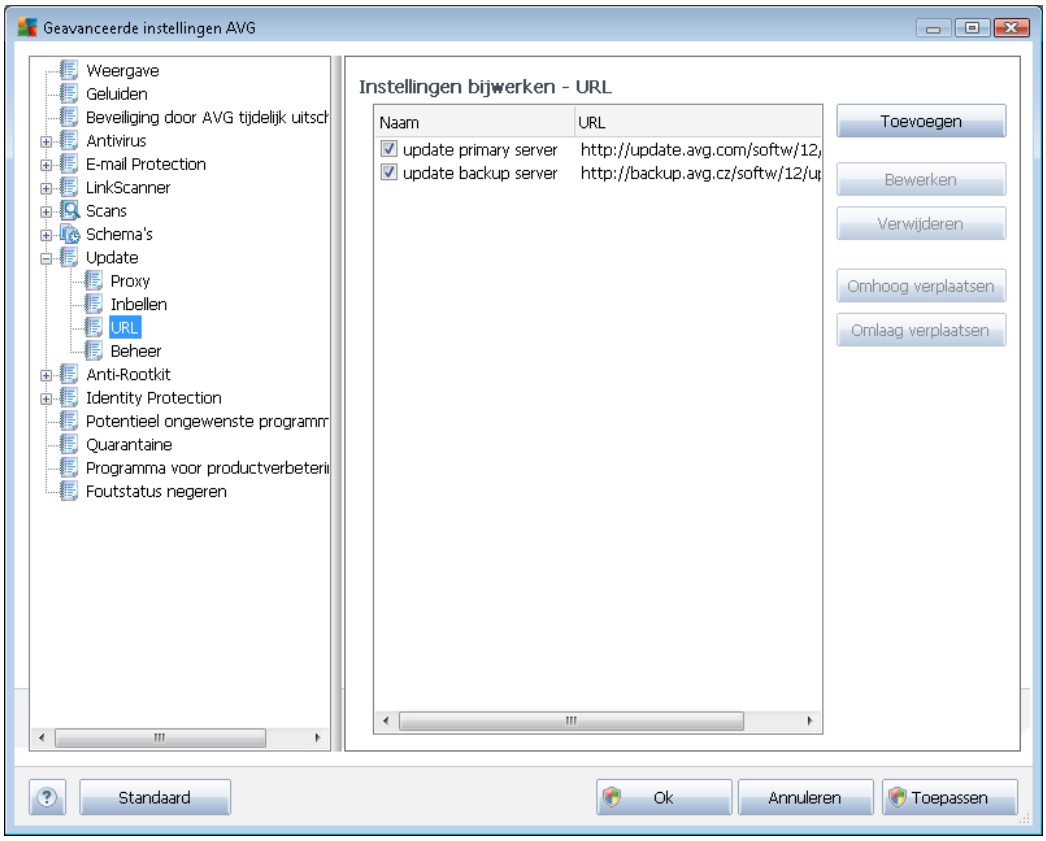
Alle parameters die optioneel zijn gedefinieerd in het dialoogvenster ***Instellingen bijwerken - Inbelverbinding*** hebben betrekking op een inbelverbinding met internet. De opties op het tabblad zijn uitgeschakeld, tenzij u het selectievakje ***Inbelverbindingen gebruiken*** inschakelt:



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***).

9.9.3. URL

In het dialoogvenster ***URL*** wordt een lijst met internetadressen weergegeven die u kunt gebruiken om de updatebestanden te downloaden:



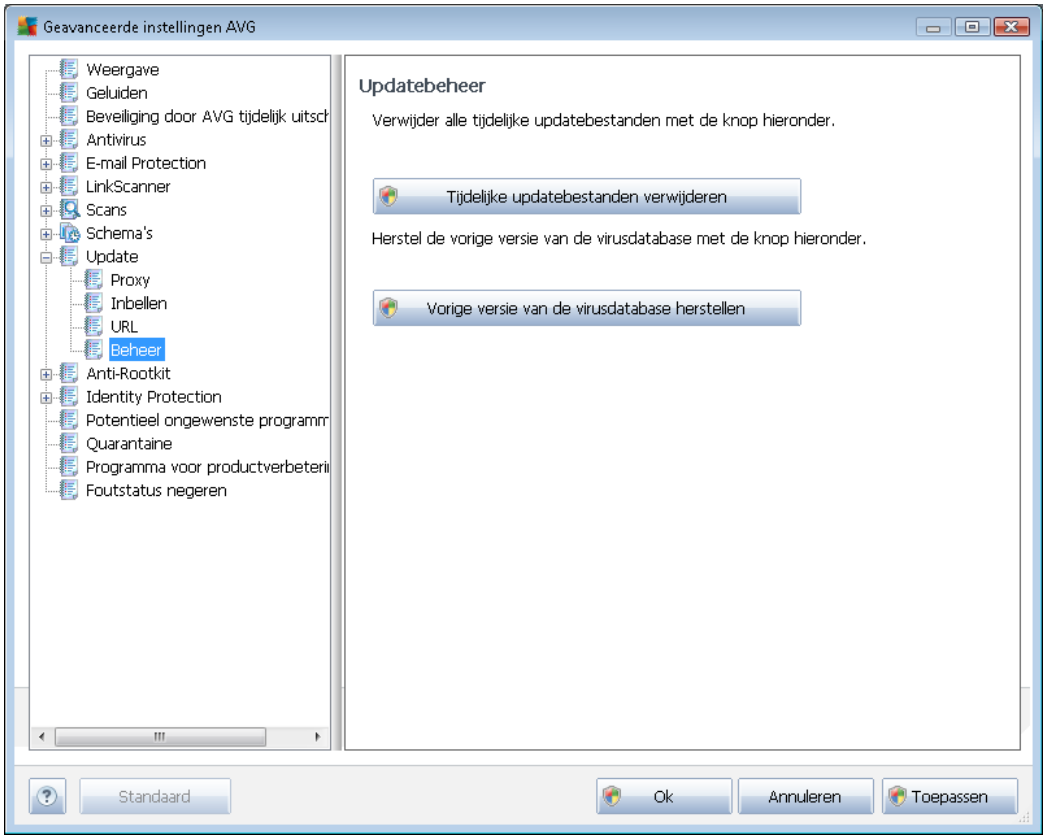
Knoppen

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

9.9.4. Beheer

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

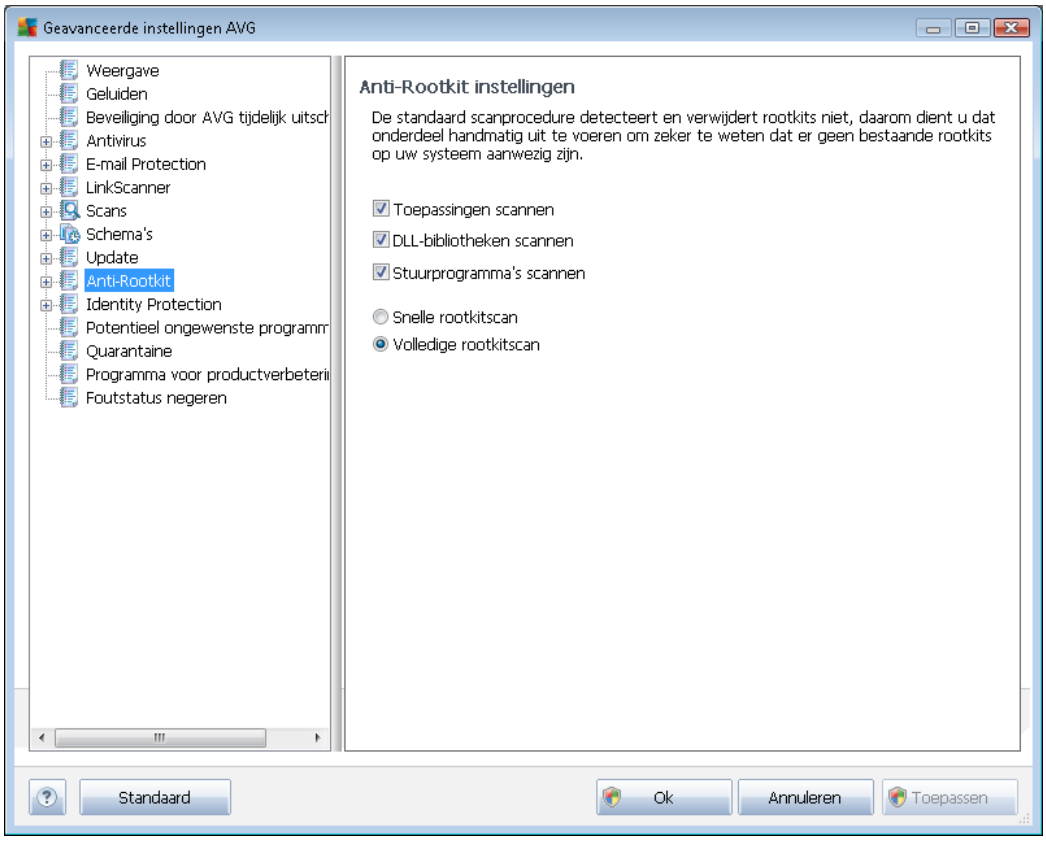


- ***Tijdelijke bestanden verwijderen*** – Klik op deze knop als u alle redundante updatebestanden wilt verwijderen van uw vaste schijf (. *Standaard worden deze bestanden 30 dagen bewaard*)

- ***Vorige versie van de virusdatabase herstellen*** – Klik op deze knop als u de nieuwste versie van de virusdatabase van uw vaste schijf wilt verwijderen en als u deze wilt vervangen door de vorige versie (*de nieuwe versie van de database wordt dan een onderdeel van de volgende update*)

9.10. Antirootkit

U kunt in het dialoogvenster ***Anti-Rootkitinstellingen*** de configuratie van het onderdeel Anti-Rootkit bewerken:



Het bewerken van alle instellingen van het onderdeel Anti-Rootkit is tevens mogelijk in het dialoogvenster dat rechtstreeks toegankelijk is vanuit de interface van het onderdeel Anti-Rootkit.

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

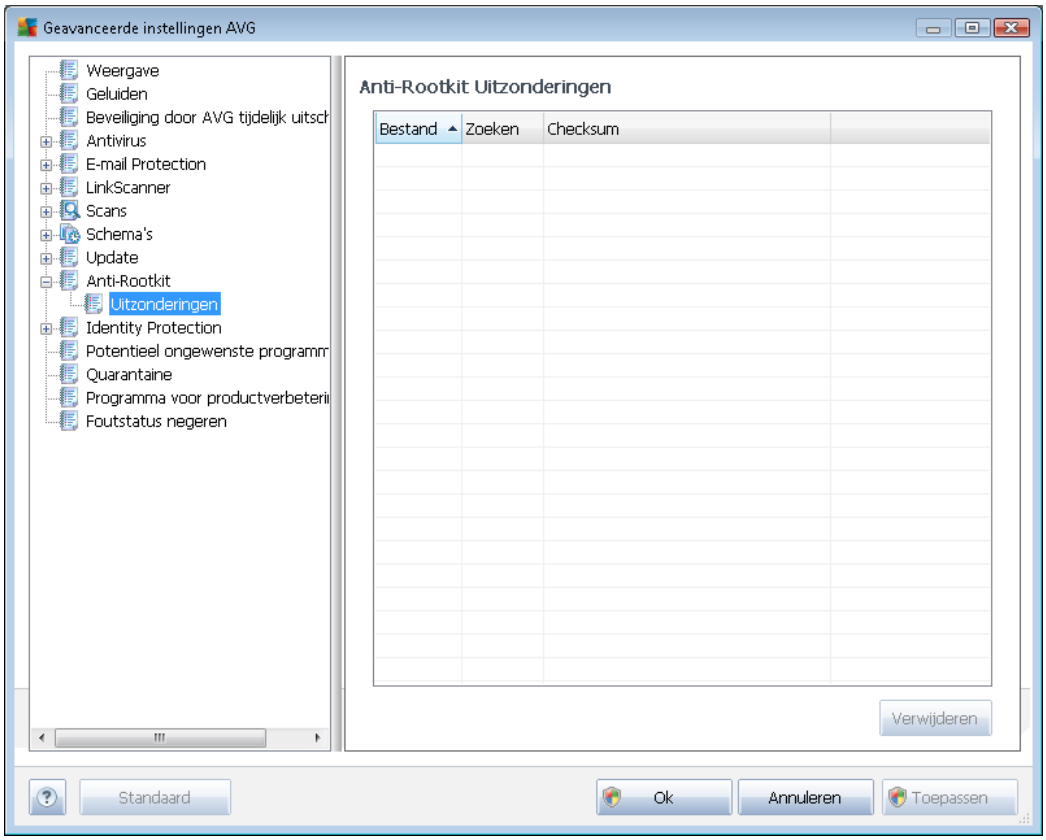
- ***Toepassingen scannen***
- ***DLL-bibliotheken scannen***
- ***Stuurprogramma's scannen***

Vervolgens kunt u de scanmodus kiezen:

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

9.10.1. Uitzonderingen

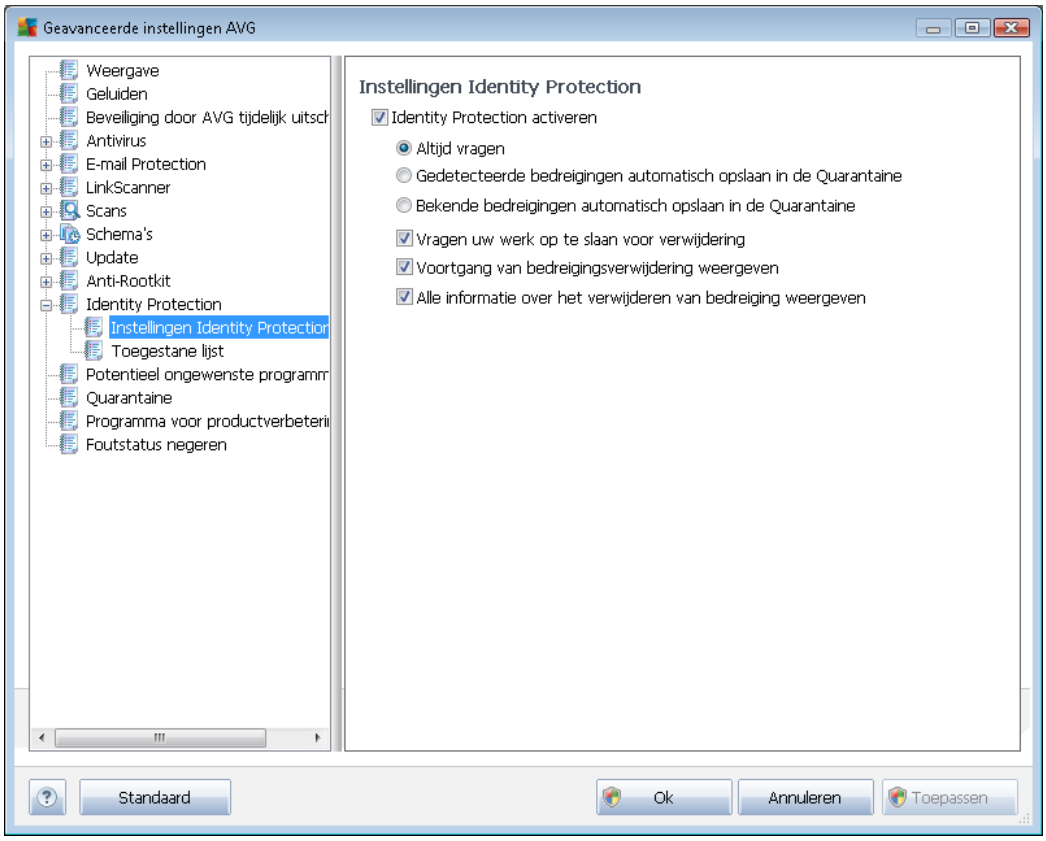
U kunt in het dialoogvenster ***Anti-Rootkit Uitzonderingen*** specifieke bestanden opgeven *(sommige stuurprogramma's worden mogelijk ten onrechte gedetecteerd als rootkits)* die bij het scannen moeten worden uitgesloten:



9.11. Identity Protection

9.11.1. 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 die u wilt uitvoeren naar de Quarantaine worden verplaatst.
- ***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 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 die u wilt uitvoeren, naar de Quarantaine worden verplaatst.
- ***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 Quarantaine worden verplaatst.

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

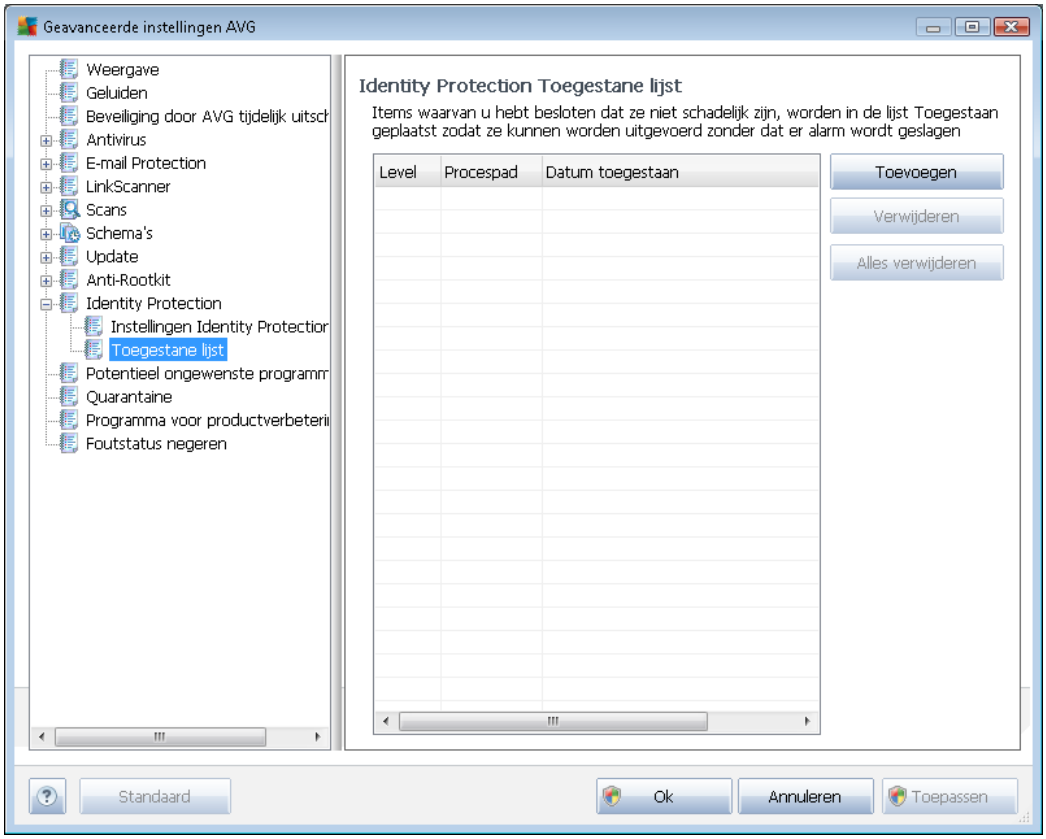
- ***Vragen uw werk op te slaan voor verwijdering*** (*standaard ingeschakeld*) – dit selectievakje moet ingeschakeld blijven als u wilt worden gewaarschuwd voordat toepassingen die worden herkend als mogelijke malware, worden verplaatst naar de Quarantaine. Als detectie plaatsvindt terwijl u met de 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.*).

9.11.2. 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 ***Identity Protection Toegestaan***, en zal hij niet opnieuw worden gerapporteerd als mogelijk gevaarlijk:



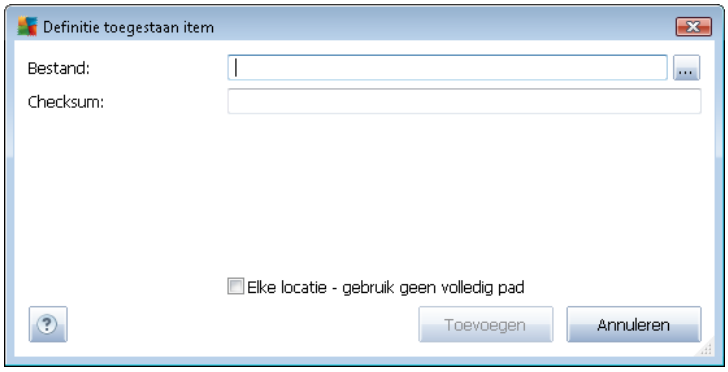
In de lijst ***Identity Protection Toegestaan*** staat de volgende informatie over elke toepassing:

- ***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 van Identity Protection*** 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:

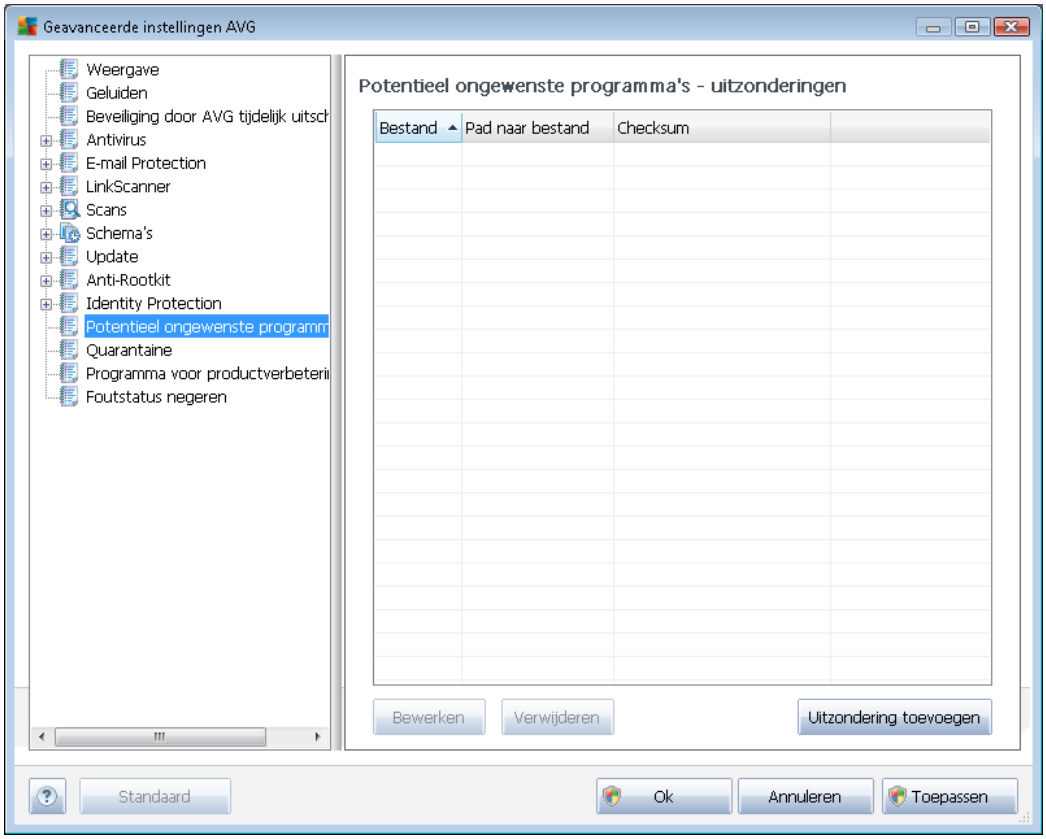


- ***Bestand*** – Typ het volledige pad naar het bestand (*de toepassing*) dat/die u als uitzondering wilt markeren
- ***Checksum*** – de unieke "handtekening" van het gekozen bestand. Deze handtekening bestaat uit een automatisch gegenereerde tekenreeks op basis waarvan AVG het gekozen bestand onmiskenbaar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

9.12. Mogelijk ongewenste programma's

AVG Anti-Virus 2012 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 Anti-Virus 2012** mogelijk gedetecteerd en gerapporteerd als een *potentieel ongewenst programma*. Als u een dergelijk programma niet van uw computer wilt verwijderen, kunt u het desbetreffende programma definiëren als een uitzondering:



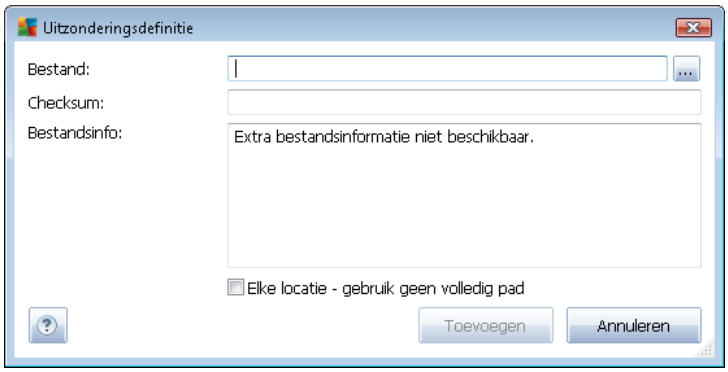
In het dialoogvenster ***Uitzonderingen voor mogelijk ongewenste programma's*** staat een lijst met eerder als zodanig gedefinieerde en geldige uitzonderingen op mogelijk ongewenste programma's. U kunt de lijst bewerken, bestaande items verwijderen en nieuwe uitzonderingen toevoegen. De volgende informatie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

- ***Bestand*** – De exacte 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

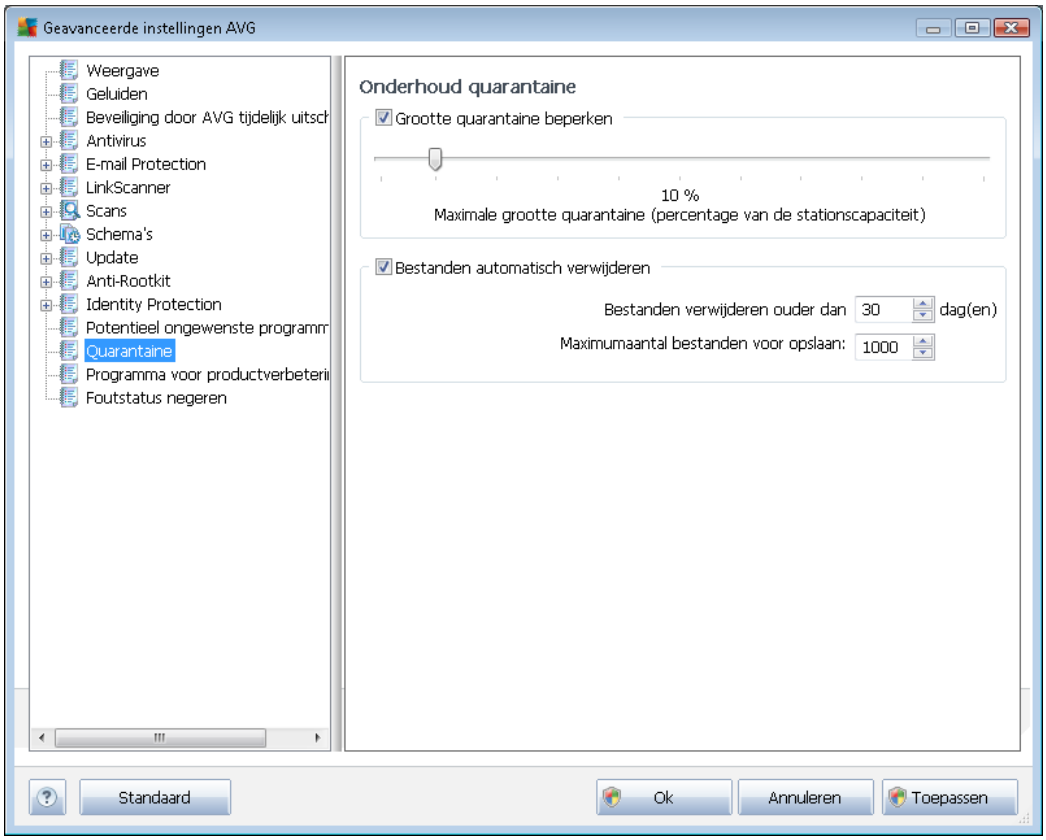
- ***Bewerken*** – er wordt een nieuw dialoogvenster geopend (*identiek met het dialoogvenster voor het toevoegen van een nieuwe uitzondering, zie hieronder*) voor het bewerken van een eerder gedefinieerde uitzondering, waarin u parameters kunt wijzigen
- ***Verwijderen*** – het geselecteerde item wordt 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.
- ***Bestandsinfo*** – Hiermee geeft u evenueel beschikbare aanvullende informatie weer over het bestand *(licentie-/versie-informatie, enzovoort)*.
- ***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. Als het selectievakje is ingeschakeld, wordt het gespecificeerde bestand gedefinieerd als een uitzondering, ongeacht op welke locatie dit zich bevindt*(. U moet echter toch het volledige pad van het bestand opgegeven. Het bestand wordt vervolgens gebruikt als een uniek voorbeeld voor het geval er twee bestanden met dezelfde naam op uw systeem staan)*.

9.13. Quarantaine



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

- ***Grootte Quarantaine beperken*** - U kunt de schuifbalk gebruiken om de grootte van het item Quarantaine in te stellen. U stelt de grootte in in verhouding tot de grootte van de lokale schijf.

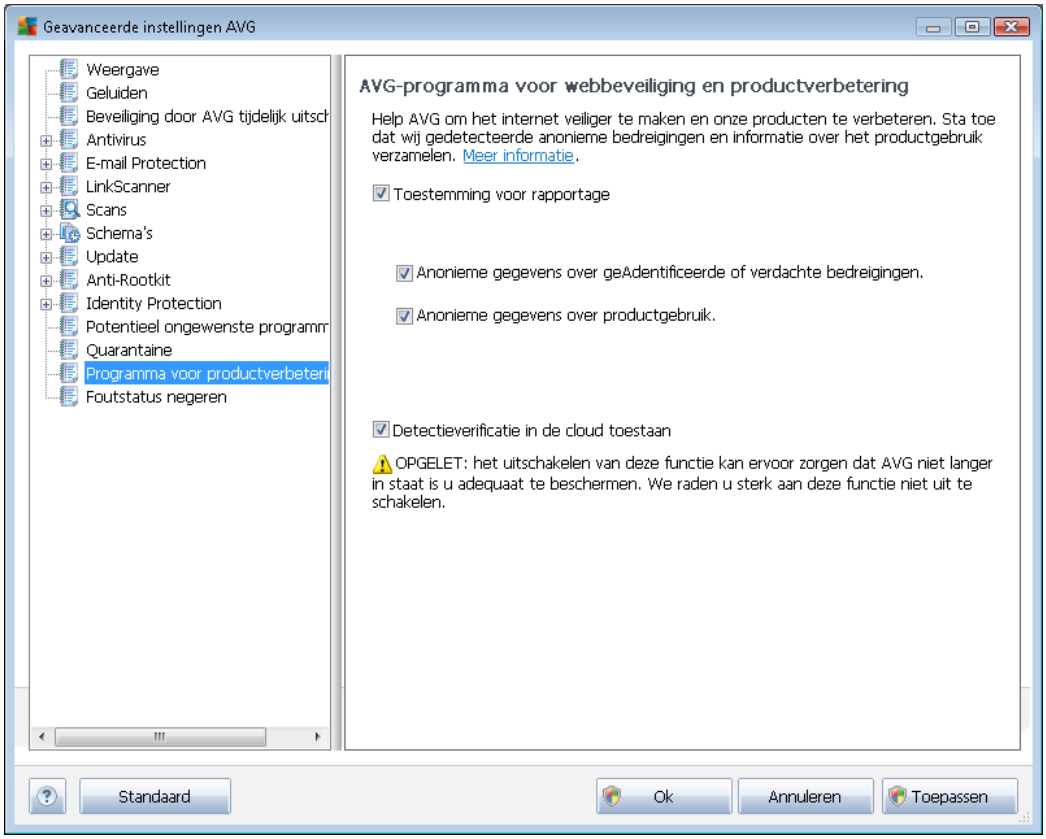
- ***Bestanden automatisch verwijderen*** - In deze sectie kunt u instellen hoe lang objecten maximaal worden opgeslagen in Quarantaine (***Bestanden verwijderen ouder dan ... dagen***) en het aantal bestanden dat maximaal wordt opgeslagen in Quarantaine (***Maximum aantal bestanden voor opslaan***).

9.14. Programma voor productverbetering

Het dialoogvenster ***AVG-programma voor webbeveiliging en productverbetering*** nodigt u uit deel te nemen aan productverbetering door AVG en ons te helpen de algehele veiligheid op internet te vergroten. Schakel de optie ***Toestemming voor rapportage*** in om rapportage van gedetecteerde bedreigingen aan AVG toe te staan. Wij kunnen dan actuele informatie over de nieuwste bedreigingen van alle deelnemers van over de hele wereld bijeen brengen en op onze beurt iedereen een betere beveiliging bieden.

Het rapporteren vindt automatisch plaats en u hebt er dus geen last van. Er wordt geen

persoonlijke informatie in de rapporten opgenomen. Het rapporteren van gedetecteerde bedreigingen is optioneel. Het wordt echter aanbevolen om deze optie ingeschakeld te laten. U helpt ons op deze wijze om de beveiliging voor u en andere AVG-gebruikers te verbeteren.



Tegenwoordig liggen er veel meer bedreigingen op de loer dan enkel virussen. De makers van kwaadaardige code en gevaarlijke websites zijn heel inventief, en nieuwe bedreigingen zien voortdurend het licht, met name via internet. Dit zijn enkele van de meest voorkomende:

- ***Een virus*** is een kwaadaardige code die zichzelf kopieert en verspreidt. Dit gebeurt vaak onopgemerkt totdat het te laat is. Sommige virussen vormen een serieuze bedreiging die de bestanden die ze tegenkomen verwijderen of opzettelijk wijzigen, terwijl andere virussen iets doen dat op het eerste gezicht onschuldig is, zoals een muziekje spelen. Maar alle virussen zijn gevaarlijk, alleen al omdat ze zich kunnen vermenigvuldigen – zelfs een gewoon virus kan in een oogwenk al het computergeheugen in beslag nemen, en een crash veroorzaken.

- ***Een worm*** behoort tot een subcategorie virussen die anders dan een normaal virus, geen "drager"-object nodig heeft waaraan het zich moet hechten. Een worm stuurt zichzelf zelfstandig door naar andere computers. Dit gebeurt gewoonlijk via e-mail. Dit resulteert vaak in overbelasting van e-mailservers en netwerksystemen.

- ***Spyware*** wordt meestal gedefinieerd als een categorie malware (*malware = kwaadaardige software, bijvoorbeeld virussen*) waartoe programma's behoren zoals trojaanse paarden die meestal bedoeld zijn om persoonlijke informatie, wachtwoorden en creditcardnummers te

stelen of om een computer te infiltreren en de aanvaller in staat te stellen deze op afstand te besturen; natuurlijk zonder dat de eigenaar van de computer dat weet of er toestemming voor heeft gegeven.

- ***Potentieel ongewenste programma's*** vormen een type spyware dat mogelijkerwijs gevaarlijk is voor uw computer. Een specifiek voorbeeld van PUP is adware, software die is ontworpen om reclame te verspreiden, meestal door pop-ups weer te geven; vervelend, maar niet meteen schadelijk.

- ***Ook tracking cookies*** kunnen worden beschouwd als een soort spyware, omdat deze kleine bestanden, die zijn opgeslagen in de browser en automatisch naar de "moeder"-website worden verstuurd als u deze weer bezoekt, data kunnen bevatten zoals uw browserhistorie en andere gelijksoortige informatie.

- ***Een Exploit*** is een kwaadaardige code die gebruikmaakt van een foutje of zwakke plek in een besturingssysteem, internetbrowser of ander essentieel programma.

- ***Phishing*** is een poging om vertrouwelijke gegevens los te peuteren door zich voor te doen als een algemeen bekende en gewaardeerde organisatie. Meestal worden de potentiële slachtoffers benaderd met een spammailtje waarin hen bijvoorbeeld gevraagd wordt hun bankgegevens bij te werken. Om dat te doen, worden ze uitgenodigd de aangeboden koppeling te volgen. Deze brengt hen vervolgens naar een imitatiewebsite van de bank.

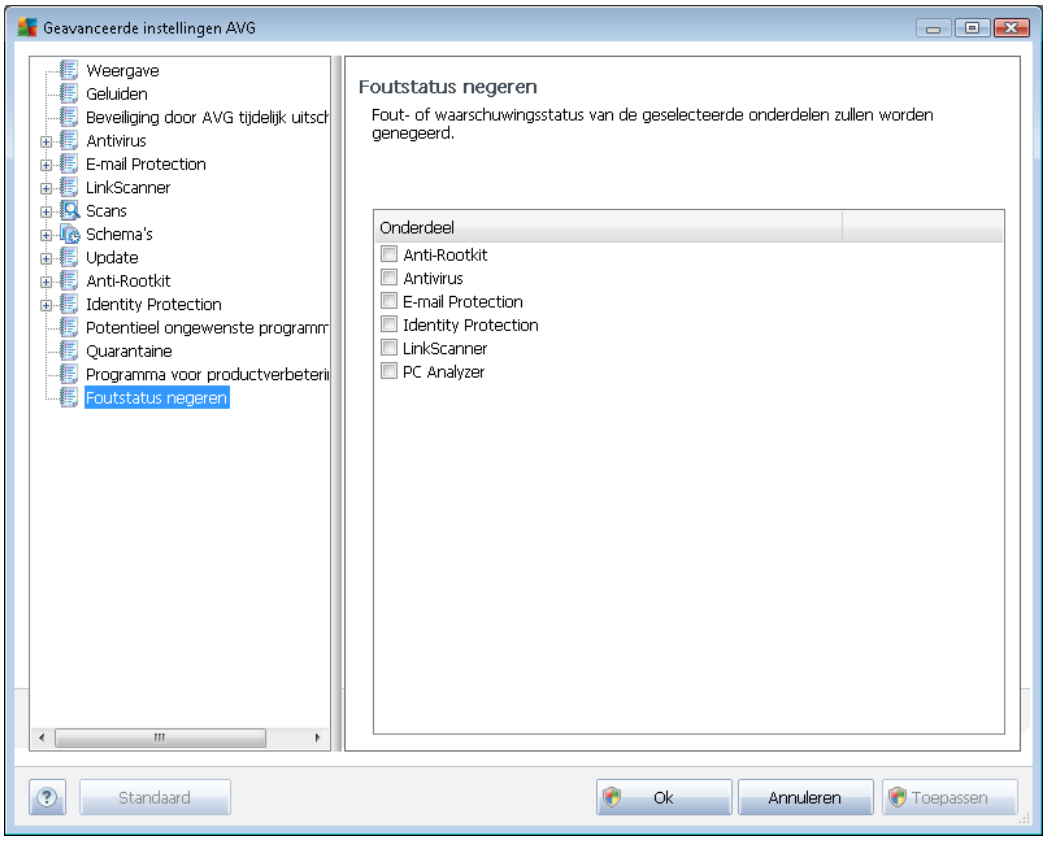
- ***Hoax is een bulke-mail die gevaarlijke, alarmerende of slechts vervelende en nutteloze informatie bevat.*** Veel van de hierboven vermelde bedreigingen maken bij de verspreiding gebruik van hoax-e-mailberichten.

- ***Kwaadaardige websites*** tenslotte, zijn websites die opzettelijk kwaadaardige software op uw computer zetten, gehackte sites doen precies hetzelfde, maar dat zijn normale (naar nu gehackte) websites die worden misbruikt om bezoekers te infecteren.

AVG Anti-Virus 2012 omvat gespecialiseerde onderdelen om u te beschermen tegen alle deze typen bedreigingen. Zie het hoofdstuk Onderdelenoverzicht voor een beknopte beschrijving daarvan.

9.15. Foutstatus negeren

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



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

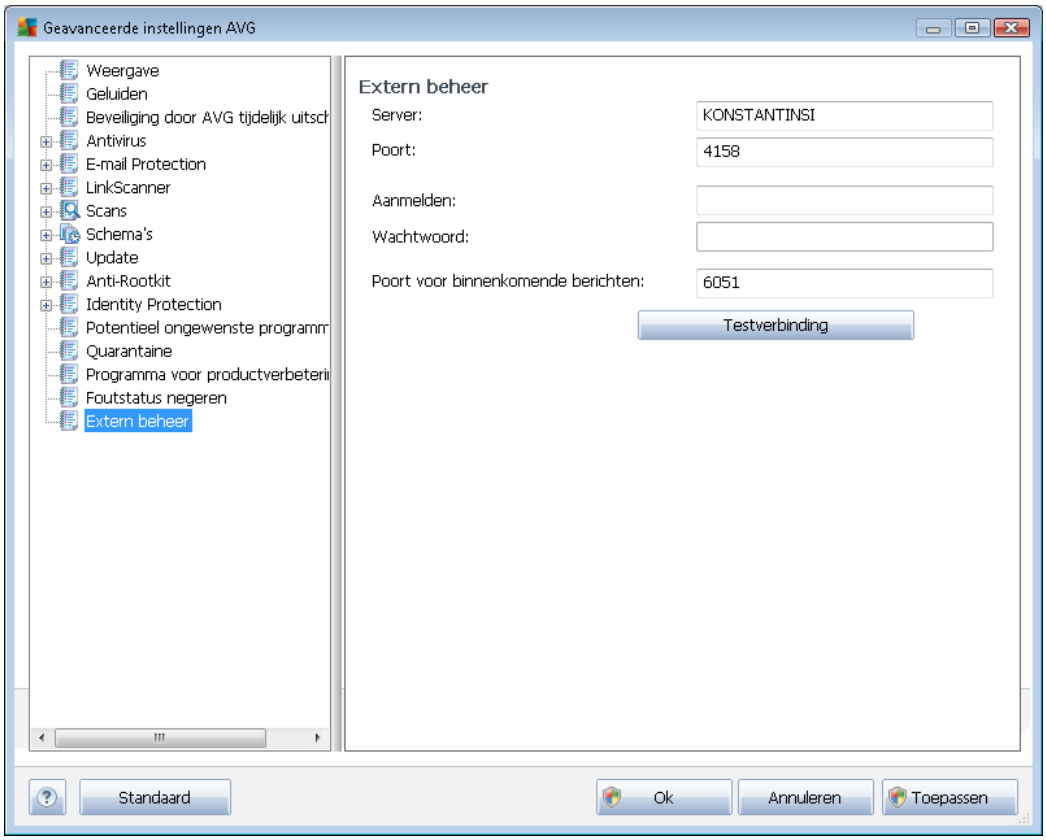
- Het systeemvakpictogram – zolang alle onderdelen van AVG correct werken, wordt het pictogram weergegeven in vier kleuren. Als er echter een fout optreedt, verschijnt er een geel uitroepteken in het pictogram,
- Een tekstbeschrijving van het huidige probleem in het gedeelte Info Beveiligingsstatus van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

Er 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 *Onderdeelstatus negeren* ook beschikbaar rechtstreeks vanuit het overzicht met onderdelen in het hoofdvenster van AVG.

9.16. Extern beheer

Het onderdeel ***Extern beheer*** en het bijbehorende dialoogvenster worden uitsluitend in de navigatiestructuur weergegeven als u **AVG Anti-Virus 2012** hebt geïnstalleerd met een AVG Business Edition-licentie en als u tijdens het installatieproces hebt bevestigd dat u het onderdeel ***Extern beheer*** wilt installeren. Zie voor een gedetailleerde beschrijving van de installatie en configuratie van Extern beheer de desbetreffende AVG Network Edition-documentatie. U kunt deze downloaden vanaf de AVG-website (http://www.avg.com/), in desectie Help / Downloaden.



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

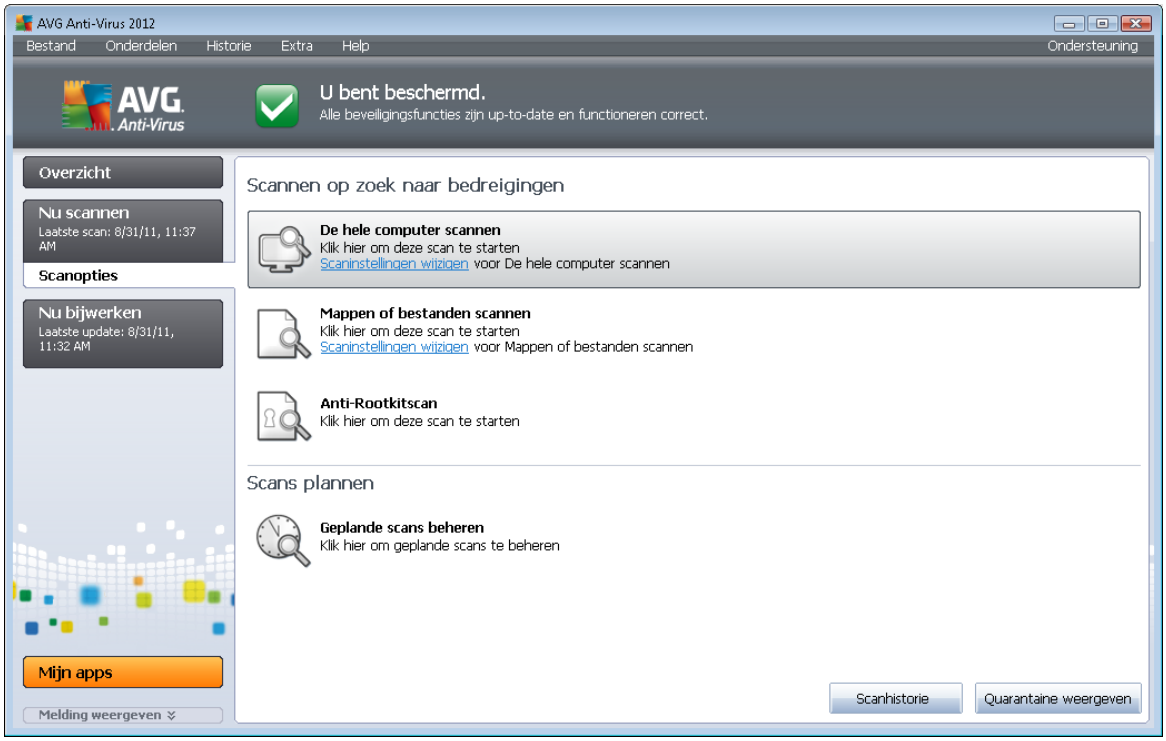
Knoppen

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.

10. AVG scannen

Standaard worden er door **AVG Anti-Virus 2012** geen scans uitgevoerd omdat de residente onderdelen van **AVG Anti-Virus 2012** na de allereerste scan zonder meer een onovertroffen bescherming bieden. Deze onderdelen zijn altijd waakzaam en blokkeren elke toegang van schadelijke code tot de computer. Natuurlijk kunt u ook een scan plannen die op basis van een ingesteld interval wordt uitgevoerd en u kunt scans handmatig starten.

10.1. Scaninterface



U kunt de scaninterface van AVG oproepen via de snelkoppeling ***Scanopties***. 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 scaninterface 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

10.2. Vooraf ingestelde scans

Een van de belangrijkste voorzieningen van **AVG Anti-Virus 2012** is de mogelijkheid om op verzoek scans uit te voeren. De scans op verzoek zijn ontworpen voor het scannen van verschillende onderdelen van uw computer in gevallen waarin u vermoedt dat er mogelijk sprake is van een virusinfectie. Het wordt met klem aangeraden om dergelijke scans regelmatig uitvoeren. Dat geldt ook als u vermoedt dat er geen virussen op uw computer zullen worden gevonden.

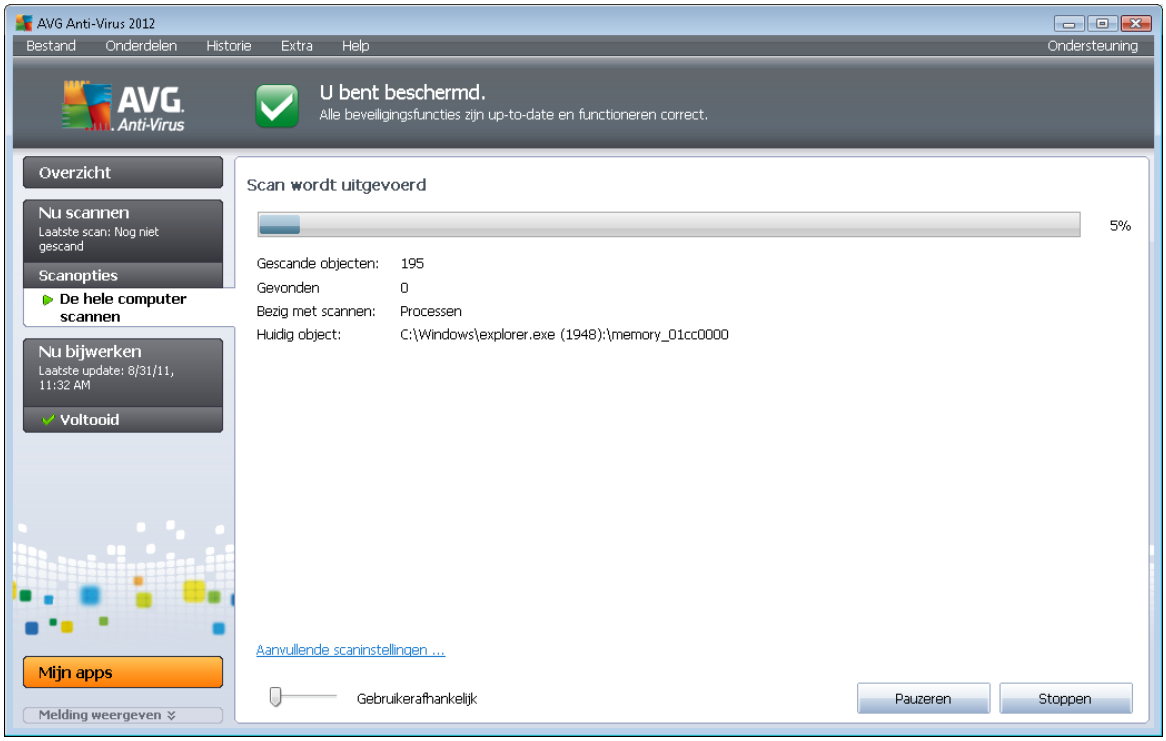
AVG Anti-Virus 2012 heeft twee scanmethodes die door de softwareleverancier van te voren zijn gedefinieerd:

10.2.1. De hele computer scannen

De hele computer scannen – de hele computer wordt gescand op mogelijk infecties en/of potentieel ongewenste programma's. 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.

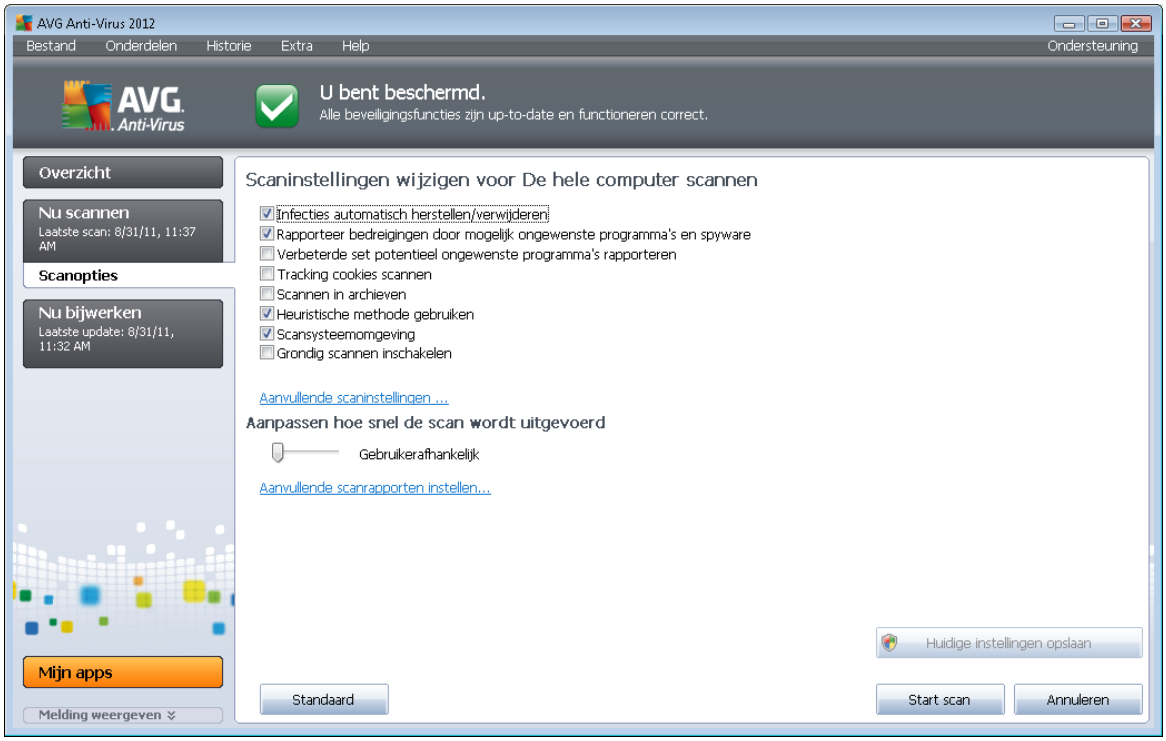
Scan starten

De scan ***De hele computer scannen*** 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

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*** *(toegankelijk vanuit de scaninterface via de koppeling Scaninstellingen wijzigen voor De hele computer scannen)*. ***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:

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

  - ***Verbeterde set potentieel ongewenste programma's rapporteren*** (*standaard uitgeschakeld*) – schakel dit selectievakje in als u pakketten die met spyware zijn uitgebreid, wilt detecteren. Dit zijn programma's die in orde en onschadelijk zijn wanneer u deze rechtstreeks van de fabrikant verkrijgt, maar die op een later tijdstip kunnen worden misbruikt voor schadelijke doeleinden. Dit is een aanvullende maatregel 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 uitgeschakeld*) – 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*).

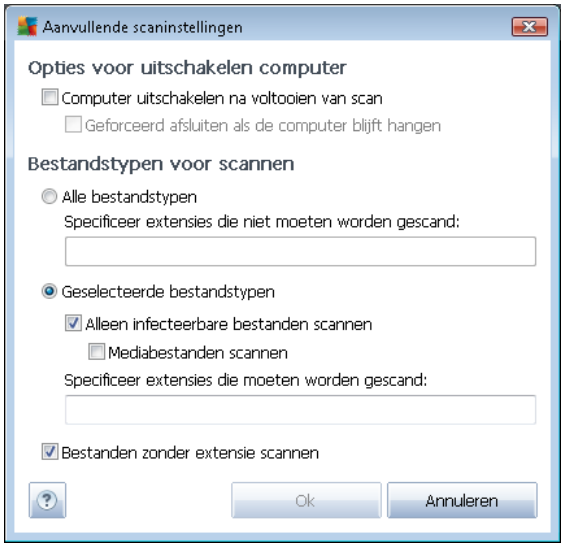
- ***Scannen in archieven*** (*standaard uitgeschakeld* – met deze parameter bepaalt u of alle bestanden moeten worden gescand, ook die bestanden die zijn gecomprimeerd in archiefbestanden, bijv. ZIP, RAR, enz.

- ***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.

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

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



- ***Opties voor uitschakelen computer*** – opgeven of de computer automatisch moet worden uitgeschakeld als het scanproces is voltooid. Als u die optie bevestigt (***Computer 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***).

- ***Bestandstypen voor scannen*** – Daarnaast moet u bepalen of u het volgende 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.

- ***De snelheid van scannen aanpassen*** – met de schuifbalk kunt u de prioriteit voor het scanproces wijzigen. Standaard is deze functie ingesteld op het niveau *gebruikerafhankelijk* voor gebruik van systeembronnen. 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.*

10.2.2. Bepaalde mappen of bestanden scannen

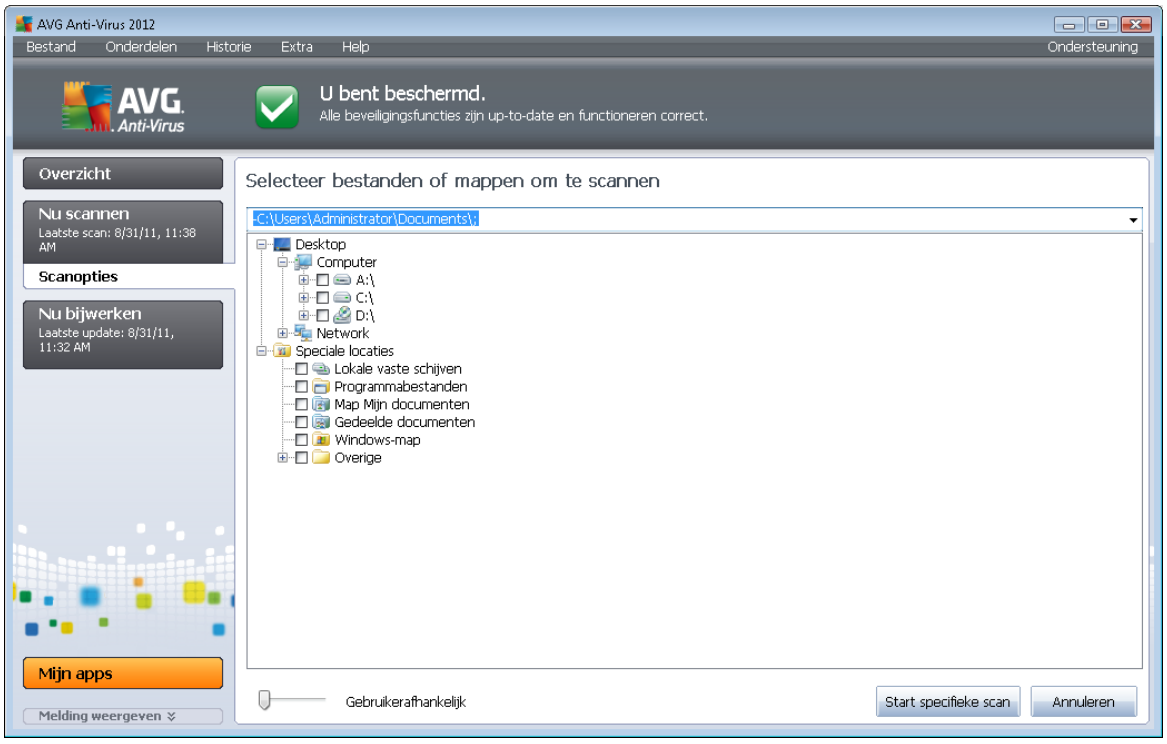
Bepaalde mappen of bestanden scannen – alleen die gebieden worden gescand die u hebt geselecteerd voor het scannen (*geselecteerde mappen, vaste schijven, diskettes, cd's, enz.*). De voortgang bij het scannen in het geval dat een virus wordt gedetecteerd, en de manier waarop het virus wordt behandeld,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

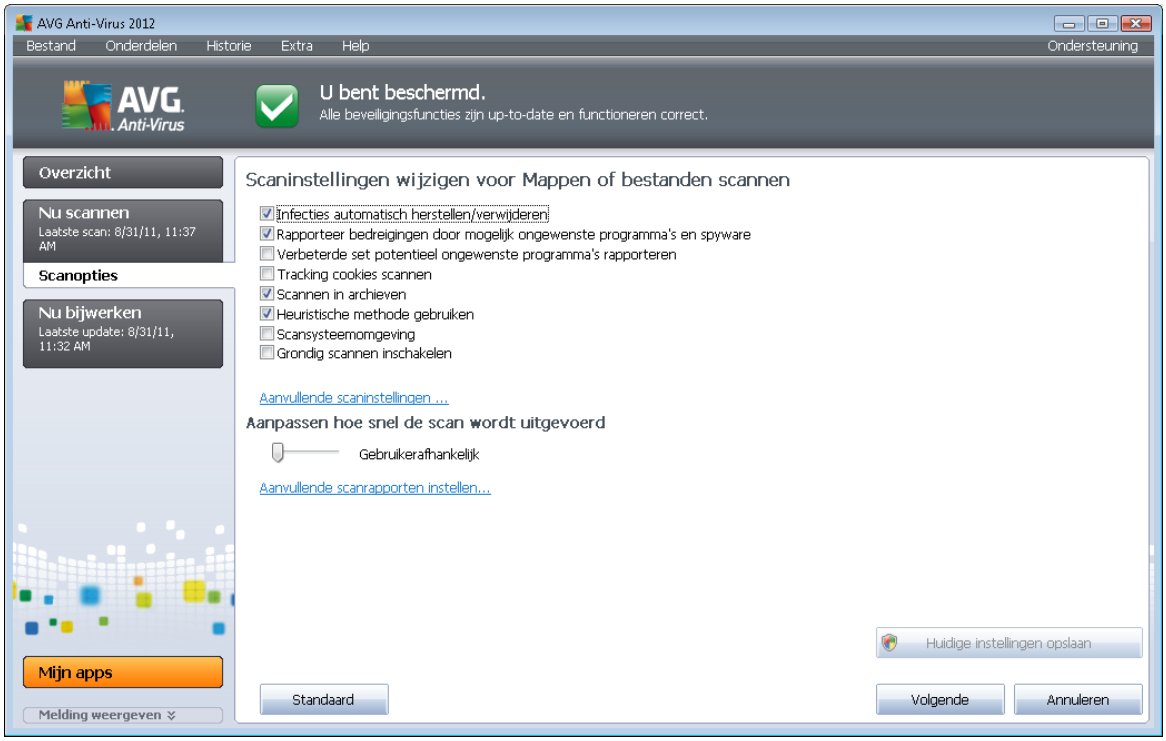
U kunt ook een map scannen, maar tegelijkertijd alle submappen van die map uitsluiten van het scannen; daartoe typt u een minteken "**-**" voor het automatisch gegenereerde pad (*zie de schermafbeelding*). Als u de hele map wilt uitsluiten van het scannen, gebruikt u de "**!**" parameter.

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 scanparameters naar wens in- en uitschakelen:

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

    - ***Verbeterde set potentieel ongewenste programma's rapporteren*** (*standaard uitgeschakeld*) – schakel dit selectievakje in als u pakketten die met spyware zijn uitgebreid, wilt detecteren. Dit zijn programma's die in orde en onschadelijk zijn wanneer u deze rechtstreeks van de fabrikant verkrijgt, maar die op een later tijdstip kunnen worden misbruikt voor schadelijke doeleinden. Dit is een aanvullende maatregel 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 uitgeschakeld*) – 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*).

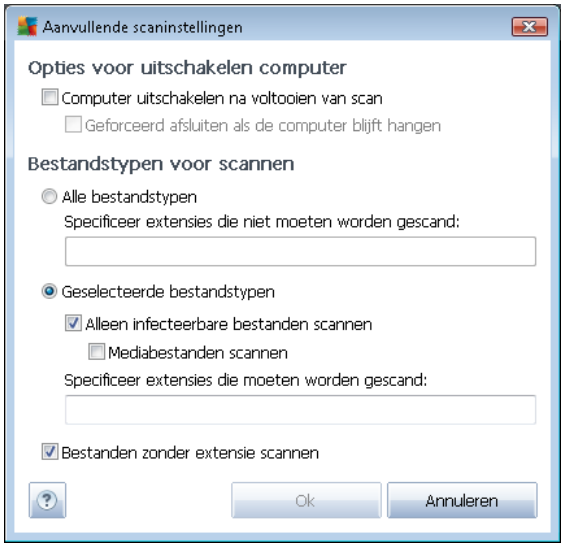
- ***Scannen in archieven*** (*standaard ingeschakeld* – met deze parameter bepaalt u of alle bestanden moeten worden gescand, ook die bestanden die zijn gecomprimeerd in archiefbestanden, bijv. ZIP, RAR, enz.

- ***Heuristische methode gebruiken*** (*standaard uitgeschakeld*) – 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 uitgeschakeld*) – als de parameter is ingeschakeld worden ook de systeemgebieden gescand.

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

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



- ***Opties voor uitschakelen computer*** – opgeven of de computer automatisch moet worden uitgeschakeld als het scanproces is voltooid. Als u die optie bevestigt (

Computer 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***).

- ***Bestandstypen voor scannen*** – Vervolgens moet u bepalen wat u 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 deze functie ingesteld op het niveau *gebruikerafhankelijk* voor gebruik van systeembronnen. 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*

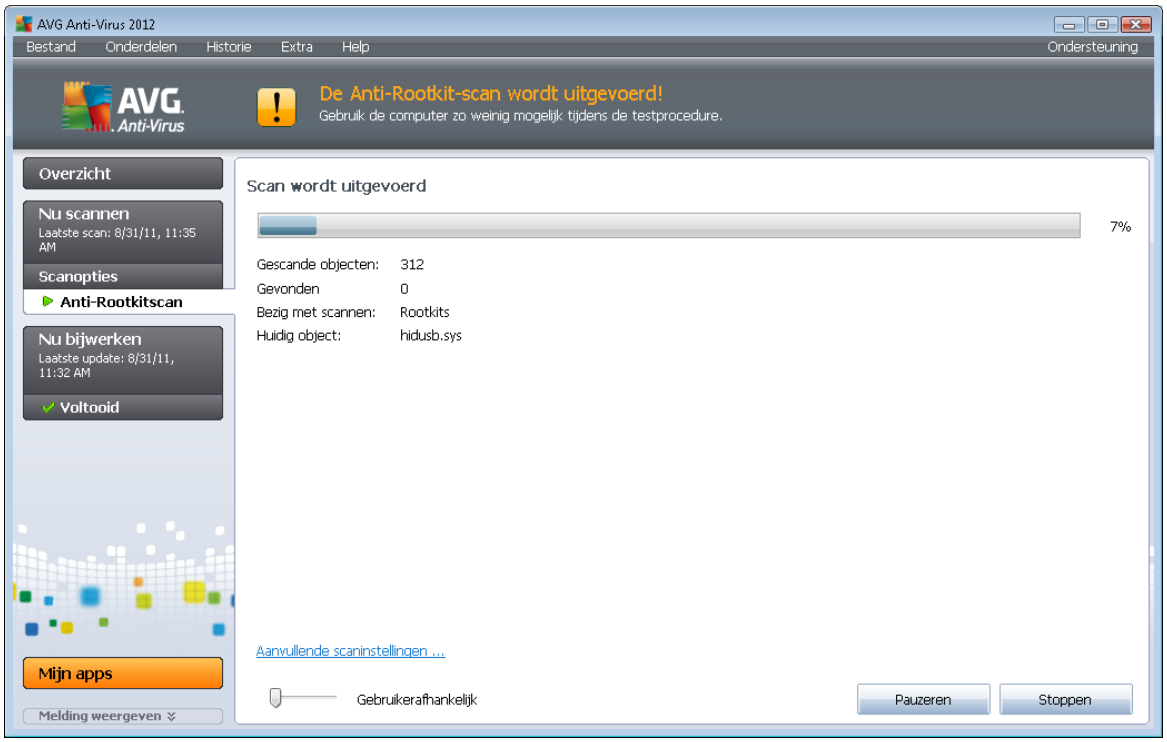
nieuwe geplande scans (alle aangepaste scans worden gebaseerd op de dan actuele configuratie van de Scan van bepaalde mappen of bestanden).

10.2.3. Antirootkitscan

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.



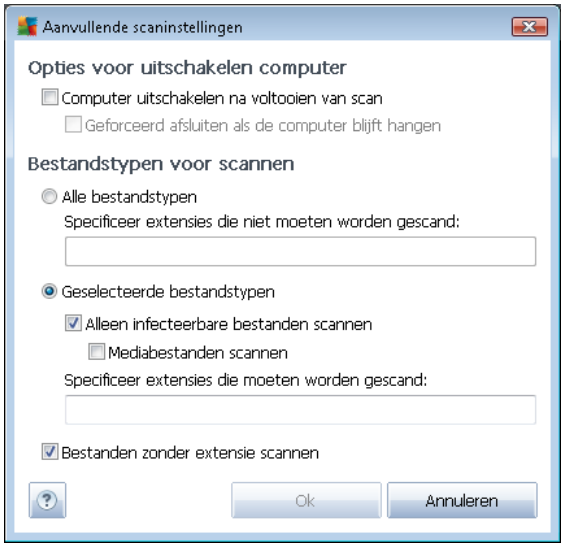
Scanconfiguratie bewerken

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 is de volgende configuratie beschikbaar, maar alleen wanneer de scan wordt uitgevoerd:

- ***Automatische scan*** – met de schuifbalk kunt u de prioriteit voor het scanproces wijzigen.

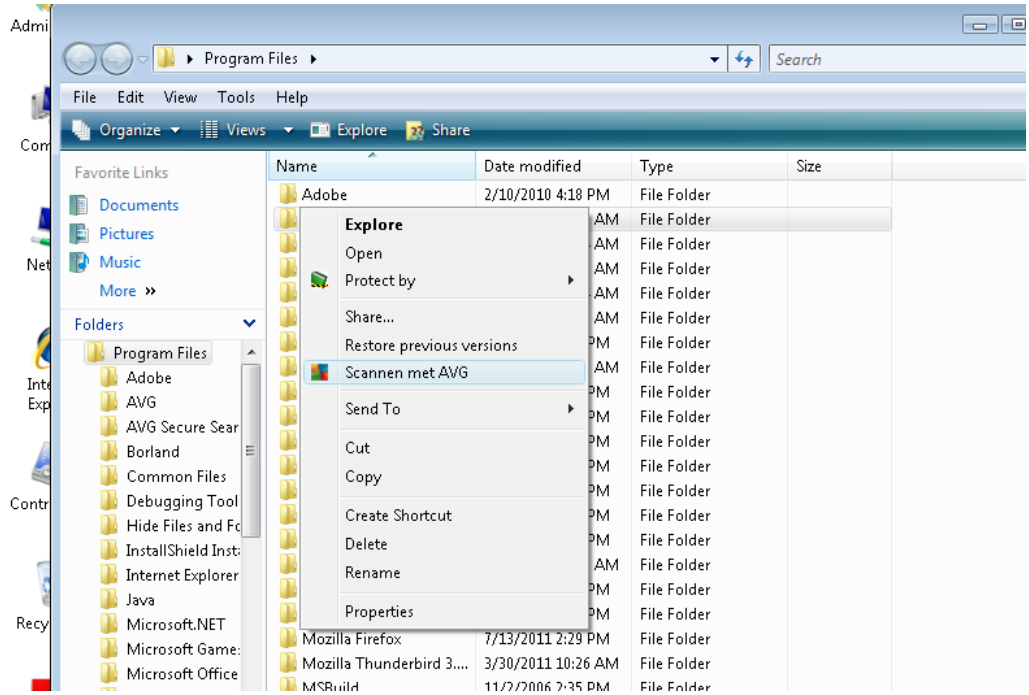
Standaard is deze functie ingesteld op het niveau *gebruikerafhankelijk* voor gebruik van systeembronnen. U kunt ook langzamer scannen, wat betekent dat een minder groot beroep wordt gedaan op systeembronnen (*dat is handig als u met de computer aan het werk bent en het u niet uitmaakt hoe lang het scanproces 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***):



10.3. 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 Anti-Virus 2012** ook snel een specifiek object scannen in Windows Verkenner. Als u een onbekend bestand wilt openen en niet zeker weet of de inhoud veilig is, kunt u het op verzoek scannen. Ga als volgt te werk:



- Selecteer in Windows Verkenner het bestand *(of de map)* dat u wilt controleren
- Klik met de rechtermuisknop op het object om het snelmenu te openen
- Kies de optie ***Scannen met AVG*** om het bestand te scannen met **AVG Anti-Virus 2012**

10.4. Scannen vanaf opdrachtregel

In **AVG Anti-Virus 2012** hebt u de mogelijkheid om een scan uit te voeren vanaf de opdrachtregel. U kunt deze optie bijvoorbeeld op servers gebruiken of voor het maken van een batch-script dat onmiddellijk na het opstarten van de computer moet worden uitgevoerd. U kunt vanaf de opdrachtregel scans starten met het merendeel van de parameters die beschikbaar zijn in de grafische gebruikersinterface van AVG.

Voer, als u AVG Scan vanaf de opdrachtregel wilt starten, de volgende opdracht uit in de map waarin AVG is geïnstalleerd:

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

Syntaxis van de opdracht

De opdracht volgt de onderstaande syntaxis:

- ***avgscanx /parameter*** ... bijv. ***avgscanx /comp*** voor het scannen van de hele computer

- ***avgscanx /parameter /parameter*** .. bij gebruik van meerdere parameters moeten deze achter elkaar worden geplaatst en van elkaar worden gescheiden door een spatie en een schuine streep (slash)

- Als een parameter bepaalde waarden vereist (zoals 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 desbetreffende opdracht gevolgd door de parameter /? of /HELP (bijv. ***avgscanx /?***). De enige verplichte parameter is /SCAN om te specificeren welke gedeelten van de computer moeten worden gescand. Voor een gedetailleerdere uitleg van de opties, raadpleegt u het overzicht van de opdrachtregelparameters.

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

CMD-scannen gestart vanuit grafische interface

Wanneer u uw computer gebruikt in 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.

10.4.1. CMD-scanparameters

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

- ***/SCAN*** Specifieke bestanden of mappen scannen */SCAN=pad;pad (bijvoorbeeld /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/

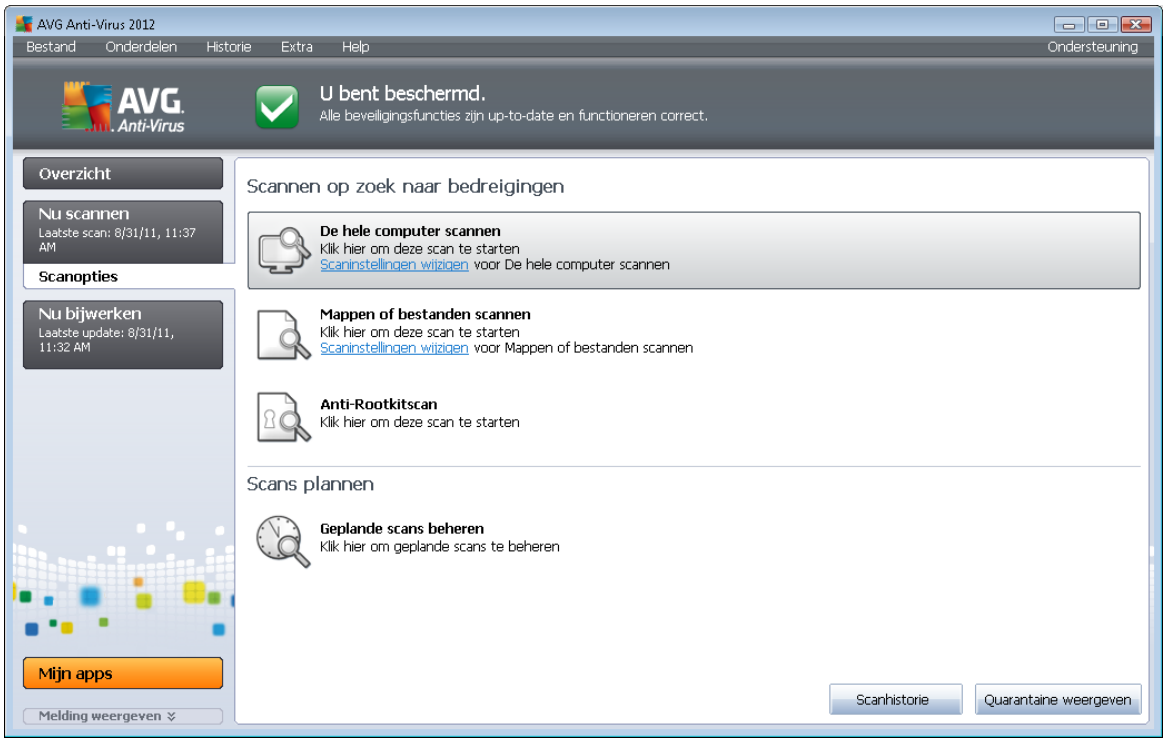
- ***/ARC*** Archieven scannen
- ***/CLEAN*** Automatisch opschonen
- ***/TRASH*** Geïnfecteerde bestanden verplaatsen naar de Quarantaine
- ***/QT*** Snelle test
- ***/MACROW*** Macro's in rapport opnemen
- ***/PWDW*** Bestanden met wachtwoordbeveiliging in rapport opnemen
- ***/IGNLOCKED*** Vergrendelde 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*** Scanprioriteit instellen /Laag, Auto, Hoog/ *(zie Geavanceerde instellingen / Scans)*
- ***/SHUTDOWN*** Computer uitschakelen na voltooien van scan
- ***/FORCESHUTDOWN*** Computer geforceerd uitschakelen na voltooien van scan
- ***/ADS*** *Alternatieve gegevensstromen scannen (alleen NTFS)*
- ***/ARCBOMBSW*** Meervoudig gecomprimeerde bestanden opnemen in rapport

10.5. Scans plannen

Met **AVG Anti-Virus 2012** 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.

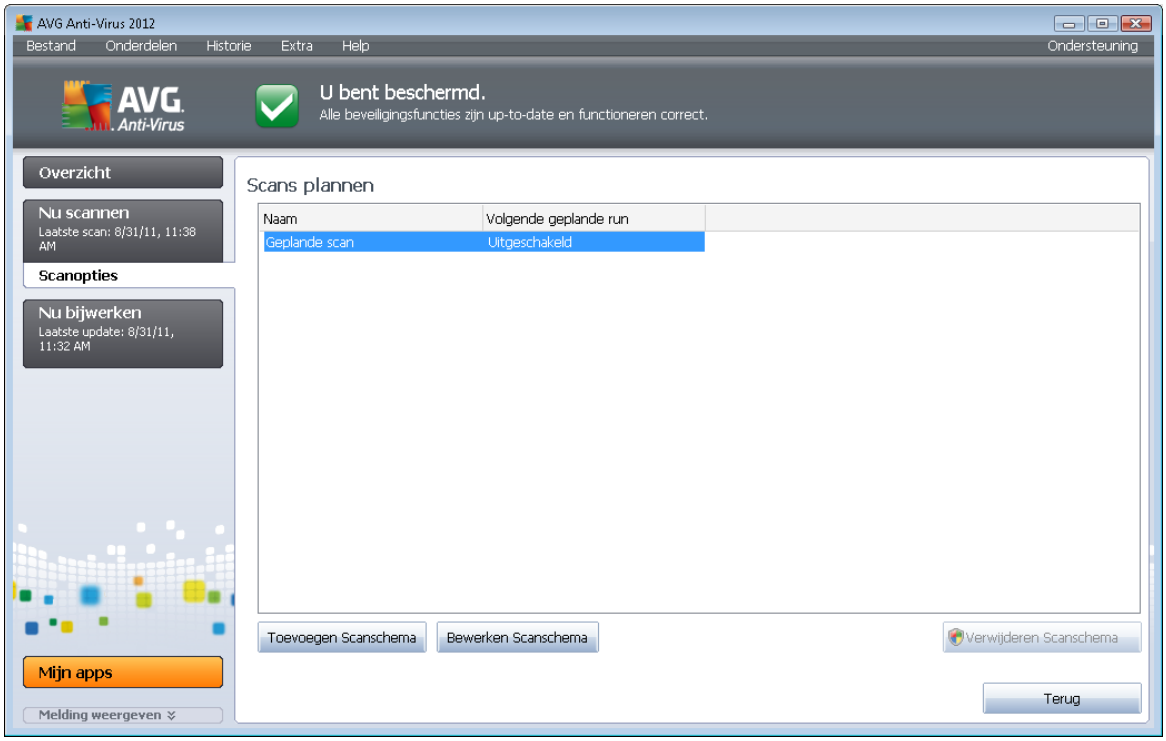
Minimaal voert u De hele computer scannen regelmatig uit, minstens één maal per week. Als het echter mogelijk is, is het verstandig om de hele computer dagelijks te scannen – zoals ook is ingesteld in de standaardconfiguratie voor scanschema's. Als de computer altijd "aan staat", kunt u de scans buiten 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 grafische pictogram in de sectie ***Scans plannen*** om een nieuw dialoogvenster ***Scans plannen*** te openen. Dit dialoogvenster bevat een lijst met alle scans die momenteel zijn gepland:



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.

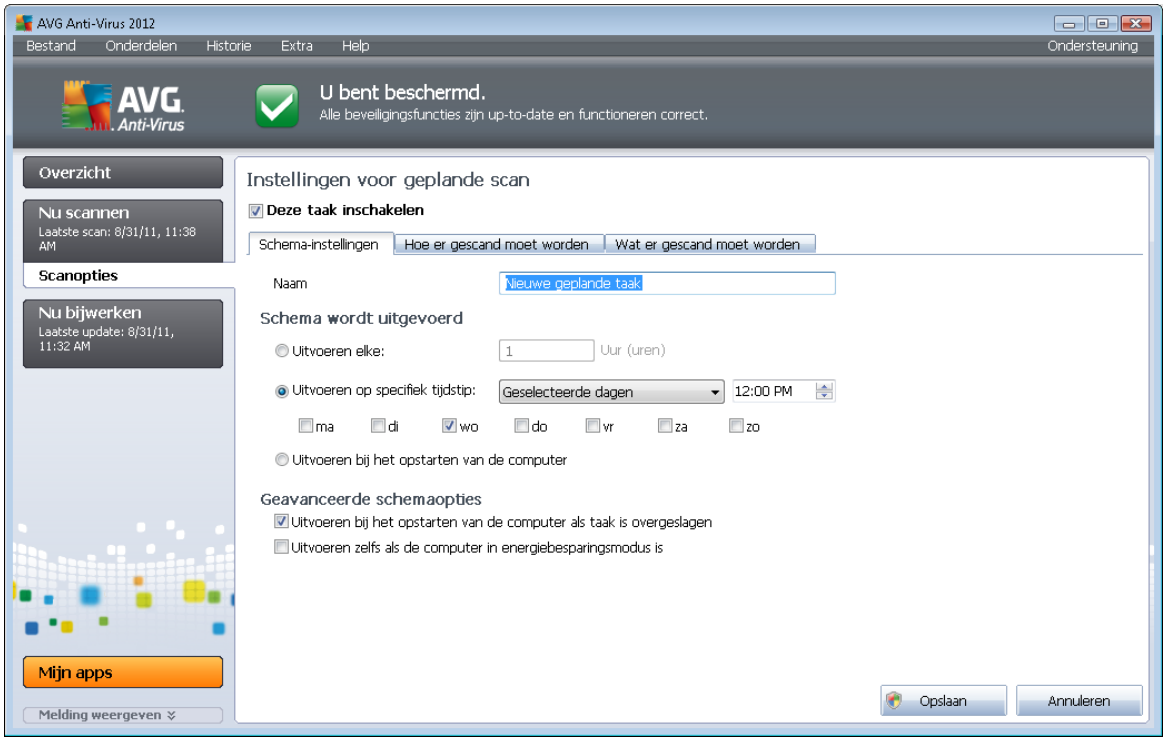
- ***Scanschema bewerken*** – deze knop is alleen actief als u eerst een bestaande scan uit de lijst met geplande scans hebt geselecteerd. In dat geval wordt de knop actief en kunt u erop klikken om het dialoogvenster ***Instellingen voor geplande scan*** te openen, met het tabblad Schema-instellingen.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

10.5.1. 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. Dit is het standaardtabblad dat automatisch wordt weergegeven*), Hoe er gescand moet worden en Wat er gescand moet worden.



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

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.

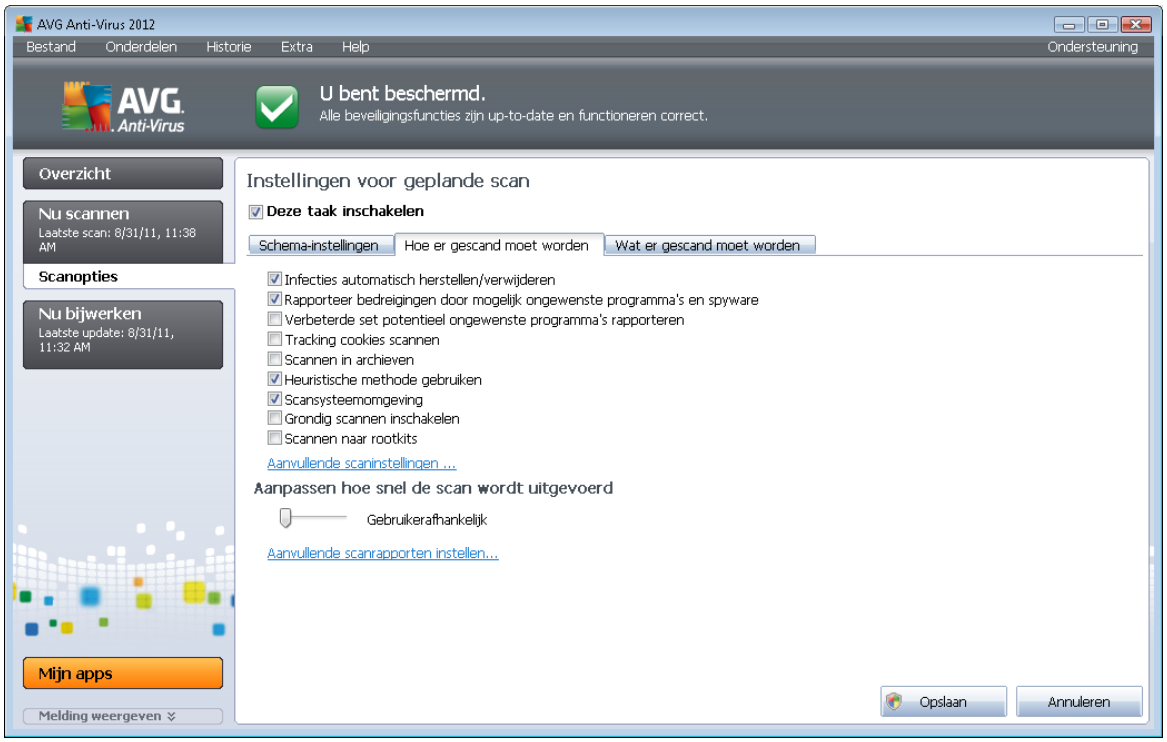
Knoppen in het dialoogvenster Instellingen voor scanschema

Alle drie de tabbladen van het dialoogvenster ***Instellingen voor scanschema*** (*Schema-instellingen, Hoe er gescand moet worden en Wat er gescand moet worden*) bevatten twee knoppen. Deze knoppen 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 scanparameters op alle drie 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.

10.5.2. 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 er tijdens

het scannen een virus wordt gedetecteerd, wordt automatisch een herstelprocedure gestart, indien deze 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.

- ***Potentieel ongewenste programma's en spywarebedreigingen rapporteren*** (*standaard ingeschakeld*) – Schakel dit selectievakje in om het Anti-Spyware-programma te activeren, zodat er op spyware en virussen kan worden gescand. Spyware behoort tot een twijfelachtige categorie malware: ook al vormt het gewoonlijk een veiligheidsrisico, sommige van deze programma's worden met opzet geïnstalleerd. Het is raadzaam deze functie niet uit te schakelen, omdat hij de bescherming van uw computer vergroot.

- ***Verbeterde set potentieel ongewenste programma's rapporteren*** (*standaard uitgeschakeld*) – Schakel dit selectievakje in als u pakketten die met spyware zijn uitgebreid, wilt detecteren. Dit zijn programma's die in orde en onschadelijk zijn wanneer u deze rechtstreeks van de fabrikant verkrijgt, maar die op een later tijdstip kunnen worden misbruikt voor schadelijke doeleinden. Dit is een aanvullende maatregel 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 uitgeschakeld*) – 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 uitgeschakeld*) – 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.

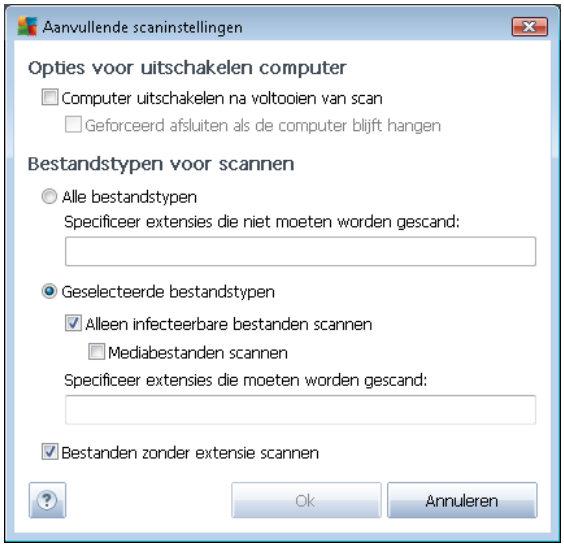
- ***Systeemgebieden scannen*** (*standaard ingeschakeld*) – als de parameter is ingeschakeld worden ook de systeemgebieden gescand.

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

- ***Scannen naar rootkits*** (*standaard uitgeschakeld*) - 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***).

  - ***Bestandstypen voor scannen*** - Daarnaast moet u bepalen of u het volgende 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.

- ***De snelheid van scannen aanpassen*** – met de schuifbalk kunt u de prioriteit voor het

scanproces wijzigen. Standaard is deze functie ingesteld op het niveau *gebruikerafhankelijk* voor gebruik van systeembronnen. 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 het dialoogvenster ***Scanrapporten*** geopend, waarin u kunt aangeven wat voor soort resultaten moeten worden gerapporteerd:

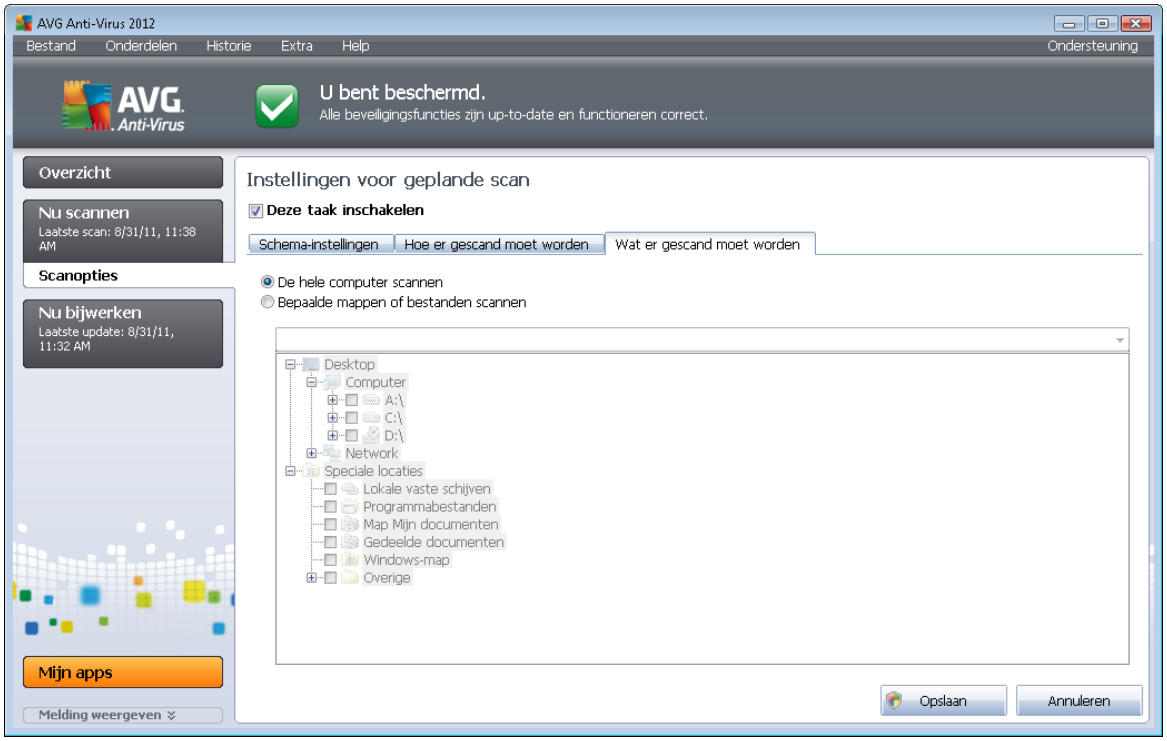
Knoppen

Alle drie de tabbladen van het dialoogvenster ***Instellingen voor scanschema*** (*Schema-instellingen*, *Hoe er gescand moet worden* en *Wat er gescand moet worden*) bevatten twee knoppen. Deze knoppen 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 scanparameters op alle drie 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.

10.5.3. 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 selectievakjes in te schakelen. De geselecteerde mappen worden weergegeven in het tekstveld boven het dialoogvenster en in de vervolgkeuzelijst wordt de geschiedenis van uw geselecteerde scans bewaard voor later gebruik. 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\
  - *in de 64-bits versie* C:\Program Files (x86)
- ***Map Mijn documenten***

- *voor Win XP:* C:\Documents and Instellingen\Default User\My Documents\
- *voor Windows Vista/7*: C:\Users\user\Documents\

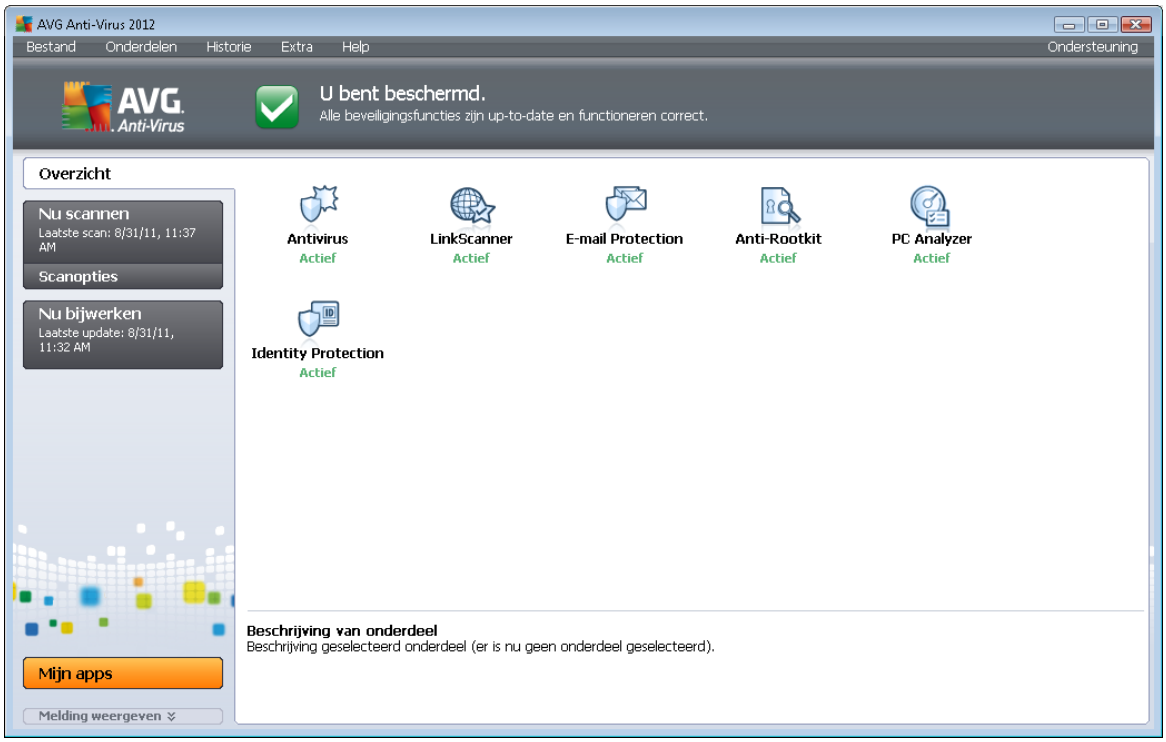
- ***Gedeelde documenten***
  - *voor Win XP*: C:\Documents and Settings\All Users\Documents\
  - *voor Windows Vista/7*: C:\Users\Public\Documents\
- ***Map Windows*** – C:\Windows\
- ***Overig***
  - *Systeemstation* – de vaste schijf waarop het besturingssysteem is geïnstalleerd (meestal C:)
  - *Systeemmap* – Windows/System32\
  - *Map tijdelijke bestanden* – C:\Documents and Settings\User\Local\ (*Windows XP*) of C:\Users\user\AppData\Local\Temp\ (*Windows Vista/7*)
  - *Tijdelijke internetbestanden* – C:\Documents and Settings\User\Local Settings\Temporary Internet Files\ (*Windows XP*) of C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files (*Windows Vista/7*)

Knoppen

Dezelfde twee knoppen zijn beschikbaar op alle drie de tabbladen van het dialoogvenster ***Instellingen voor geplande scan*** *(Schema-instellingen, Hoe er gescand moet worden en Wat er gescand moet worden)*:

- ***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 scanparameters op alle drie 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.

10.6. 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

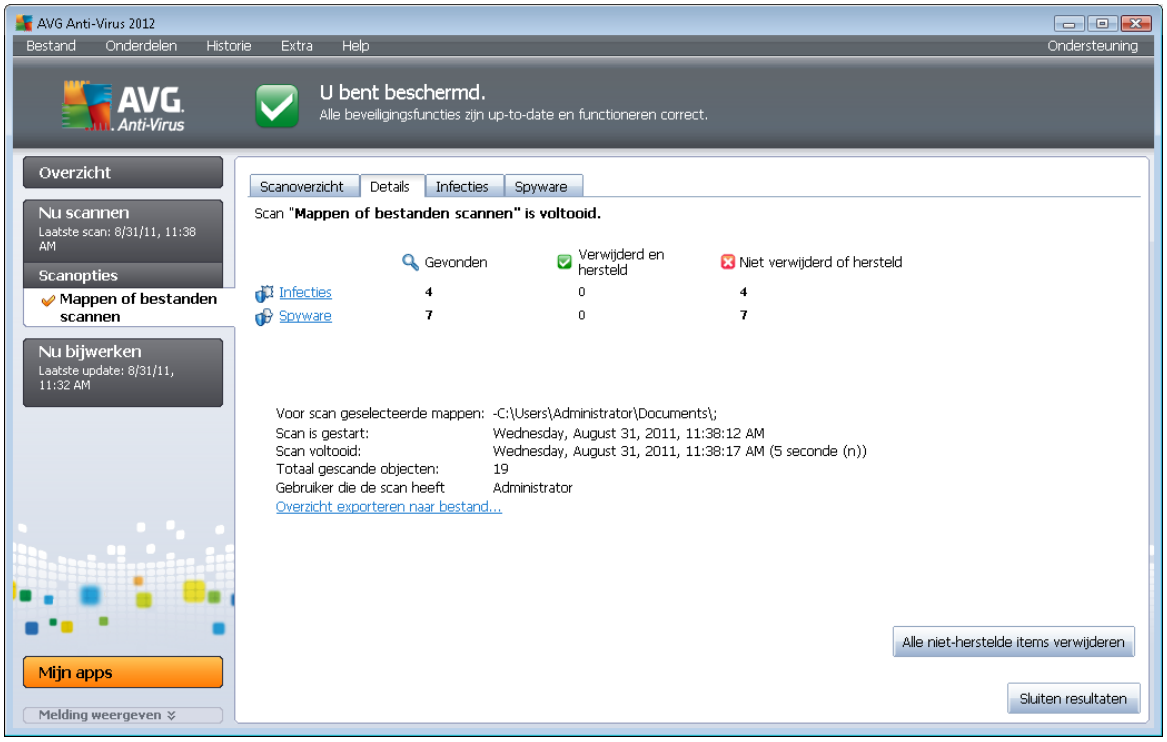
10.7. Details scanresultaten

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 verder 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 er een virusinfectie is gedetecteerd tijdens het scannen
- Spyware - Dit tabblad wordt alleen weergegeven als er spyware is gedetecteerd tijdens het scannen
- Waarschuwingen - Dit tabblad 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 een dergelijk 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 *(zoals archieven die met een wachtwoord zijn beveiligd)*.

10.7.1. Tabblad Overzicht resultaten



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

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

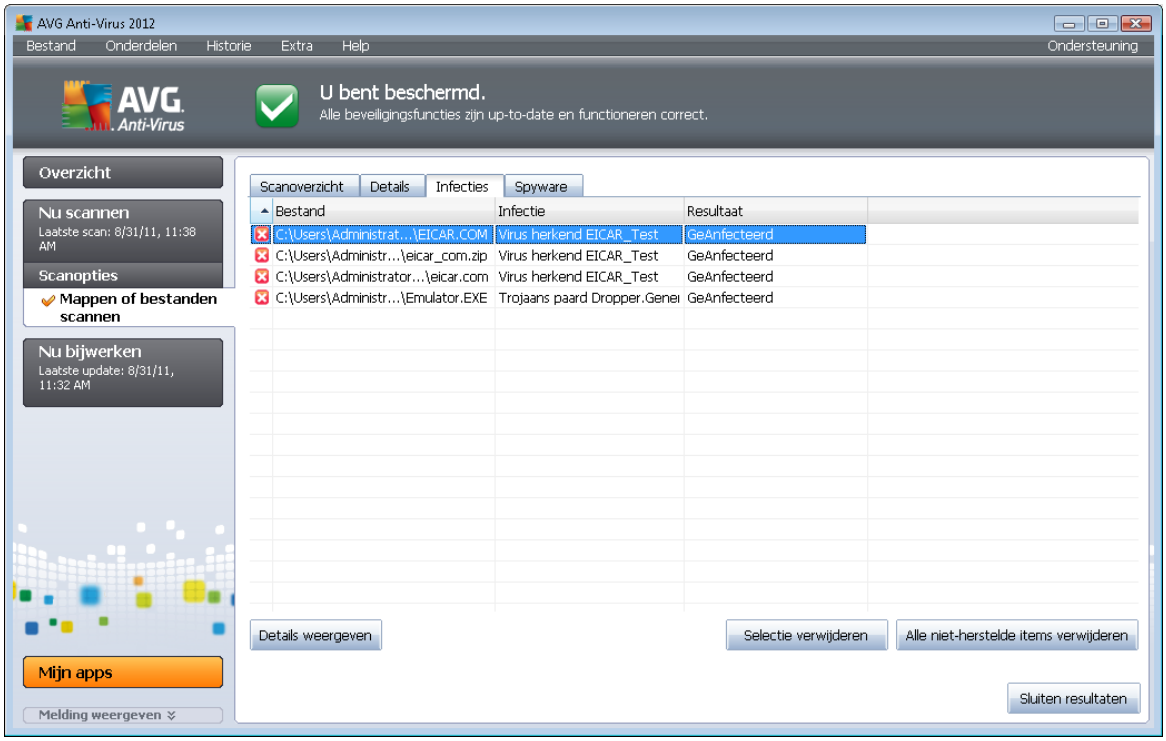
Bovendien staat er informatie over de datum en het precieze tijdstip waarop de scan is uitgevoerd, het totale aantal gescande objecten, de duur van de scan en het aantal fouten dat tijdens het scannen is opgetreden.

Knoppen

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

AVG Anti-Virus 2012 © 2011 Copyright AVG Technologies CZ, s.r.o. Alle rechten voorbehouden.

10.7.2. 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 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

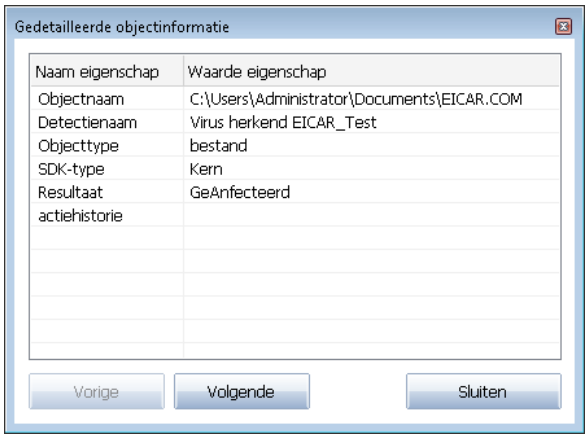
object tot de uitzonderingen behoort en het object is toegevoegd aan de lijst met PUP-uitzonderingen *(geconfigureerd bij de PUP-uitzonderingen in het dialoogvenster Geavanceerde instellingen*

- ***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:

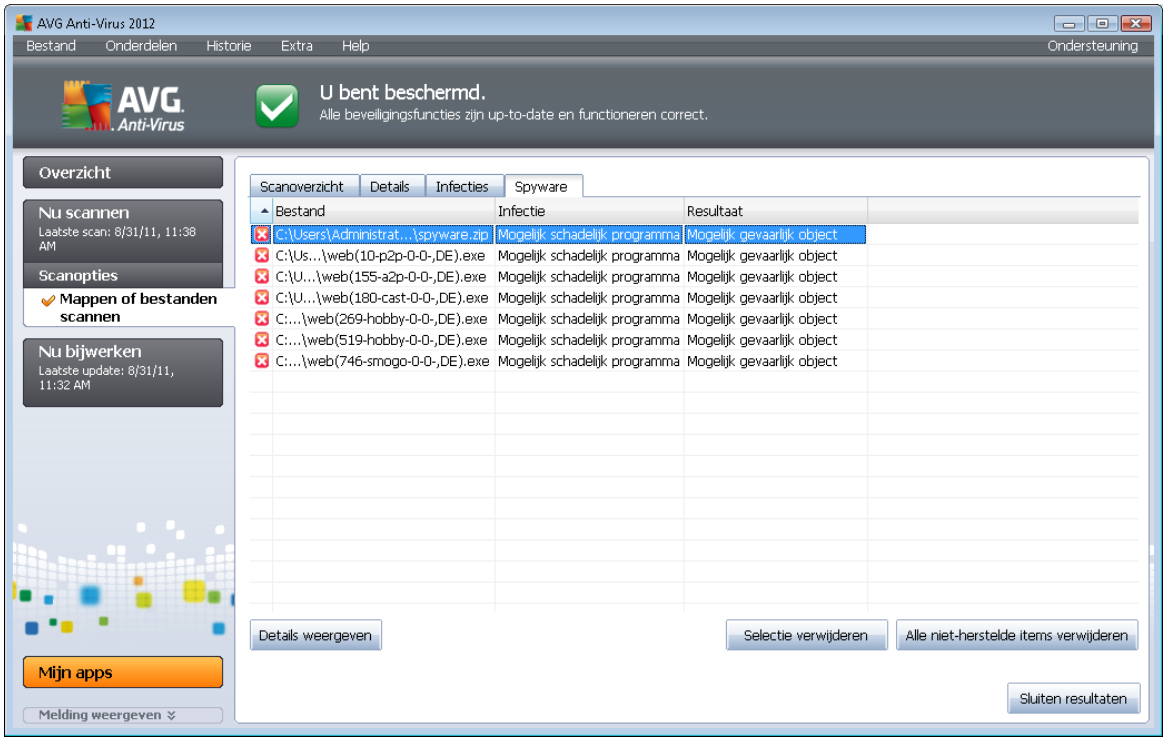


In dit dialoogvenster staat gedetailleerde informatie over het gedetecteerde geïnfecteerde object (*bijv. naam, locatie, type van het object, SDK-type, detectieresultaat en actiehistorie met betrekking tot het gedetecteerde object*. Gebruik de knoppen ***Vorige*** / ***Volgende*** om informatie te bekijken over specifieke resultaten. Met de knop ***Sluiten*** sluit u het dialoogvenster weer.

- ***Geselecteerde infecties verwijderen*** – het geselecteerde object verplaatsen naar de Quarantaine
- ***Alle niet-herstelde infecties verwijderen*** – alle objecten verwijderen die niet kunnen worden hersteld of verplaatst naar de Quarantaine
- ***Sluiten*** – het dialoogvenster sluiten en terugkeren naar het dialoogvenster Overzicht

scanresultaten

10.7.3. Tabblad Spyware



Het tabblad ***Spyware*** wordt uitsluitend weergegeven in het dialoogvenster ***Scanresultaten*** als tijdens het scannen 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 (*zie 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 in een specifieke scanconfiguratie)*
    - ***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

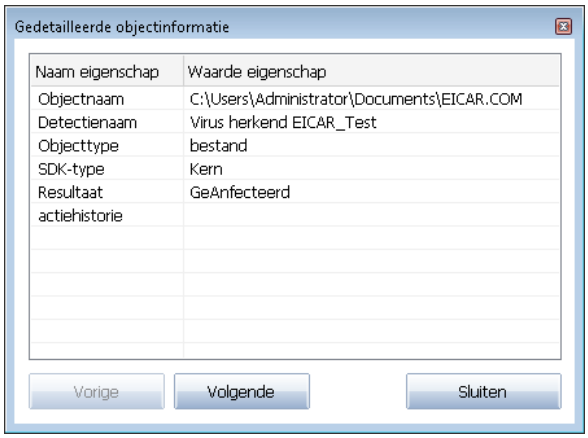
object tot de uitzonderingen behoort en het object is toegevoegd aan de lijst met PUP-uitzonderingen *(geconfigureerd bij de PUP-uitzonderingen in het dialoogvenster Geavanceerde instellingen*

- ***Vergrendeld bestand – niet gescand*** – 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 dit dialoogvenster staat gedetailleerde informatie over het gedetecteerde geïnfecteerde object (*bijv. naam, locatie, type van het object, SDK-type, detectieresultaat en actiehistorie met betrekking tot het gedetecteerde object*. Gebruik de knoppen ***Vorige*** / ***Volgende*** om informatie te bekijken over specifieke resultaten. Met de knop ***Sluiten*** sluit u het dialoogvenster weer.

- ***Geselecteerde infecties verwijderen*** – het geselecteerde object verplaatsen naar de Quarantaine
- ***Alle niet-herstelde infecties verwijderen*** – alle objecten verwijderen die niet kunnen worden hersteld of verplaatst naar de Quarantaine
- ***Sluiten*** – het dialoogvenster sluiten en terugkeren naar het dialoogvenster Overzicht

scanresultaten

10.7.4. 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 uit de testresultaten blijkt dat er uitsluitend waarschuwingen zijn gedetecteerd door **AVG Anti-Virus 2012**, is er geen 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 Anti-Virus 2012** er een verborgen bestand wordt gerapporteerd dat u verdacht of kwaadaardig voorkomt, kunt u het verplaatsen naar het item 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.

10.7.5. Tabblad Rootkits

Op het tabblad ***Rootkits*** staat informatie over rootkits die tijdens het scannen zijn gedetecteerd als u de Anti-Rootkit scan hebt gestart.

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.

10.7.6. 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 Anti-Virus 2012** is in staat om bestanden te detecteren die niet zijn geïnfecteerd, maar die wel verdacht zijn. Dergelijke 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 Anti-Virus 2012** (*en door andere anti-malwareprogramma's*) niet worden gescand.

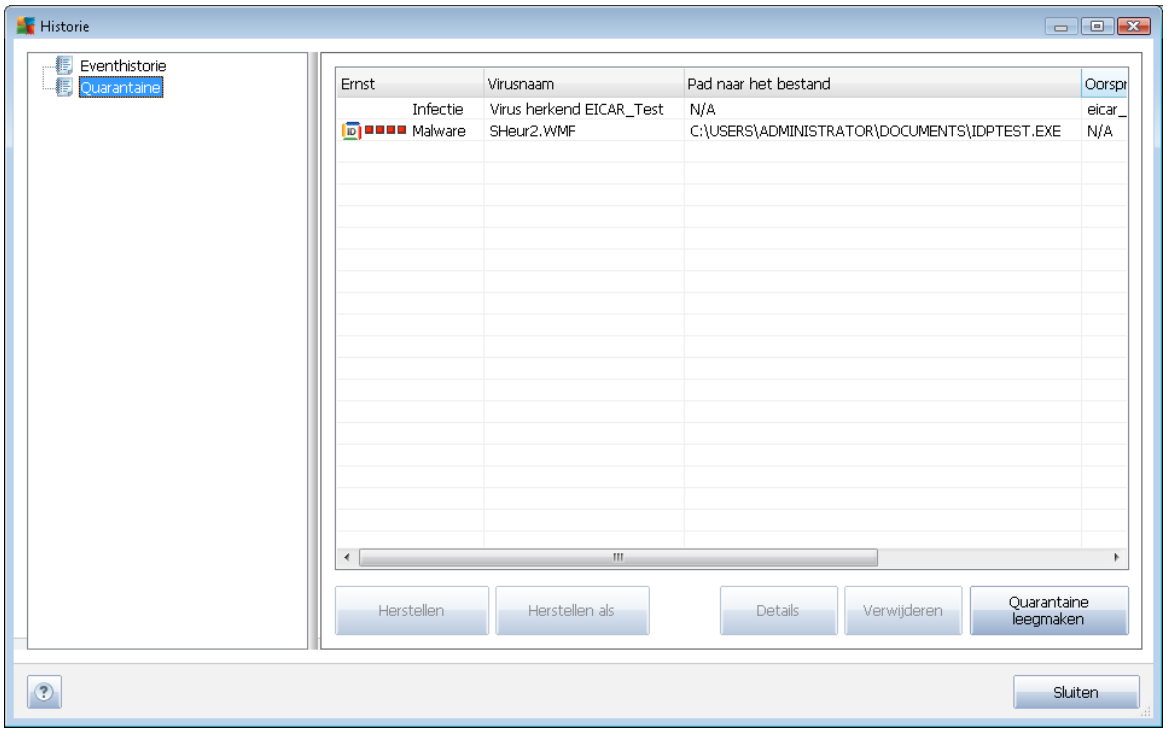
- ***Document met macro's*** - Het gerapporteerde document bevat macro's die kwaadaardig kunnen zijn.

- ***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. **AVG Anti-Virus 2012** rapporteert dergelijke bestanden om te voorkomen dat deze 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 Anti-Virus 2012** gemeld. In sommige gevallen gebruiken virussen de namen van standaardprocessen om hun aanwezigheid op het systeem te maskeren.

- ***Vergrendeld bestand*** - Het gerapporteerde bestand is vergrendeld en kan dus door **AVG Anti-Virus 2012** niet worden gescand. Dat betekent meestal dat een bestand voortdurend wordt gebruikt door het systeem (*zoals het geval is bij het wisselbestand*).

10.8. Quarantaine



Quarantaine voorziet in een veilige omgeving voor het beheren van verdachte of geïnfecteerde objecten die tijdens AVG-scans zijn gedetecteerd. Als er tijdens het scannen een geïnfecteerd object wordt gedetecteerd, wordt u gevraagd wat er met het verdachte object moet gebeuren als het desbetreffende object niet automatisch kan worden hersteld. Het wordt aanbevolen om het object in een dergelijk geval naar de ***Quarantaine*** te verplaatsen, zodat het daar kan worden afgehandeld. Het hoofddoel van de ***Quarantaine*** is elk verwijderde bestand gedurende een bepaalde periode te bewaren, zodat u zich ervan kunt vergewissen dat u het bestand niet langer nodig hebt op de oorspronkelijke locatie. Mocht het ontbreken van het bestand problemen veroorzaken, dan kunt u het 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 Anti-Virus 2012** 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

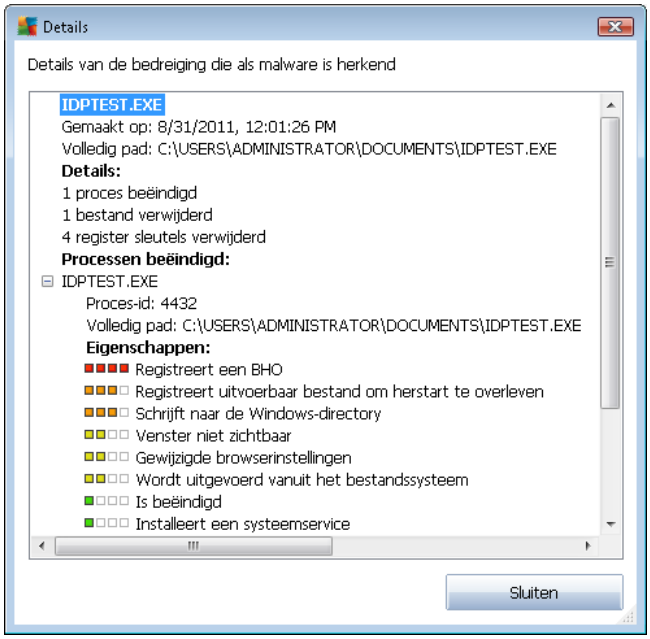
Knoppen

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

- ***Herstellen*** – het geïnfecteerde bestand wordt teruggeplaatst op de oorspronkelijke locatie

- ***Herstellen als*** – het geïnfecteerde bestand verplaatsen naar een geselecteerde map

- ***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*).

11. AVG Updates

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

Gezien het aantal nieuwe computerbedreigingen en de snelheid waarmee deze zich verspreiden, is het van essentieel belang dat u **AVG Anti-Virus 2012** regelmatig bijwerkt. Dit kunt u het beste doen door de standaardinstellingen van het programma, waarbij er automatische updates worden uitgevoerd, te behouden. Houd er rekening mee dat de meest recente bedreigingen niet door het programma kunnen worden gedetecteerd als de virusdatabase van **AVG Anti-Virus 2012** niet is bijgewerkt.

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

11.1. Update starten

AVG Anti-Virus 2012 controleert standaard om de vier uur of er nieuwe updates beschikbaar zijn, zodat er een maximale beveiliging kan worden geboden. Aangezien AVG-updates niet volgens een vast schema worden uitgebracht, maar eerder in reactie op de hoeveelheid bedreigingen en de ernst daarvan, is deze controle van groot belang om ervoor te zorgen dat de AVG-virusdatabase altijd is bijgewerkt.

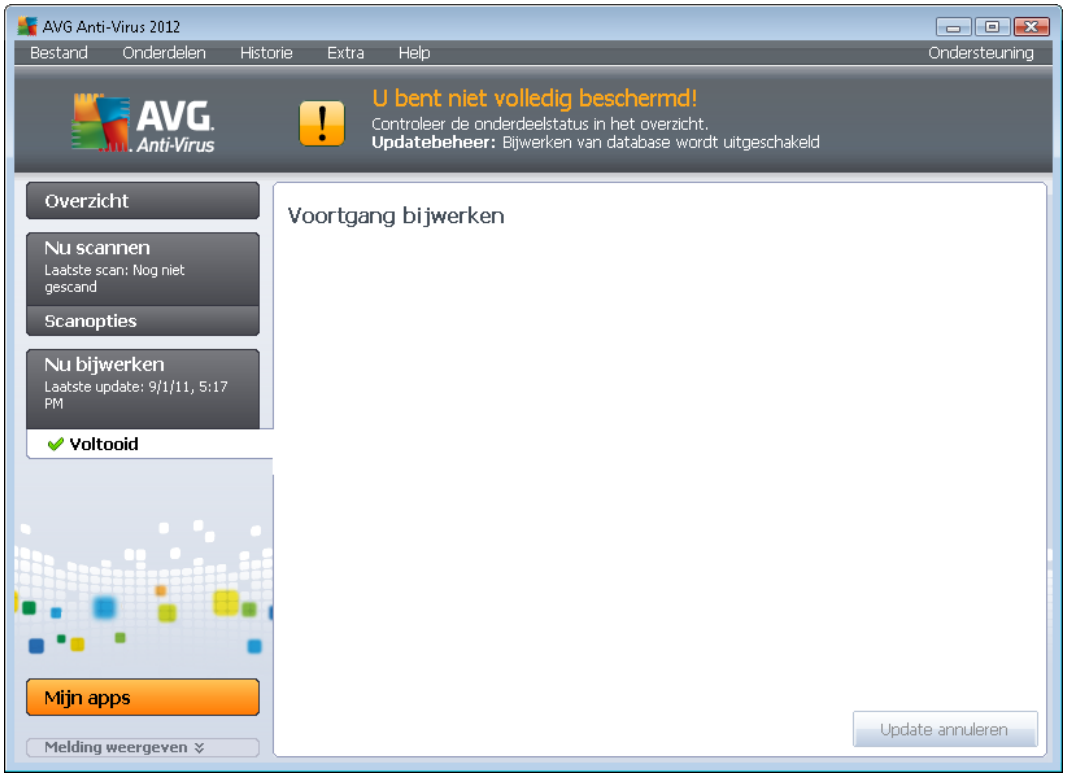
Als u het aantal keren dat het controleren op updates wordt gestart, wilt verlagen, kunt u daartoe uw eigen parameters instellen. Het wordt echter met klem aangeraden om ten minste één keer per dag een update te starten. Deze configuratie kan worden bewerkt in de sectie Geavanceerde instellingen/ Schema's. Dit gebeurt in de volgende dialoogvensters:

- Schema definitie-updates
- Updateschema programma

Als u onmiddellijk wilt controleren of er nieuwe updates beschikbaar zijn, kunt u de koppeling Nu bijwerken in de hoofdgebruikersinterface gebruiken. Deze koppeling is altijd toegankelijk vanuit alle dialoogvensters van de gebruikersinterface.

11.2. Voortgang van update

Als u de updateprocedure start, wordt eerst gecontroleerd of er nieuwe updates beschikbaar zijn. Als dat het geval is, start **AVG Anti-Virus 2012** het downloaden en de updateprocedure. Tijdens het uitvoeren van de updateprocedure wordt het dialoogvenster ***Update*** geopend waarin op een grafische wijze de voortgang wordt weergegeven. Dit dialoogvenster biedt verder een overzicht van relevante statistische parameters (*grootte updatebestand, ontvangen gegevens, downloadsnelheid, verstreken tijd, …*):



***Opmerking**: voorafgaande aan het starten van de AVG-programma-update wordt er een systeemherstelpunt gemaakt. Als de updateprocedure faalt en uw besturingssysteem beschadigd raakt, kunt u uw besturingssysteem altijd herstellen in de oorspronkelijke configuratie vanaf dit punt. Deze optie is toegankelijk via het Windows-menu Start / Alle programma's / Accessoires / Systeemprogramma's / Systeemherstel. Alleen aanbevolen voor ervaren gebruikers.*

11.3. Updateniveaus

U kunt in **AVG Anti-Virus 2012** kiezen uit twee updateniveaus:

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

- ***Update van programma*** bevat diverse programmawijzigingen, reparaties en verbeteringen.

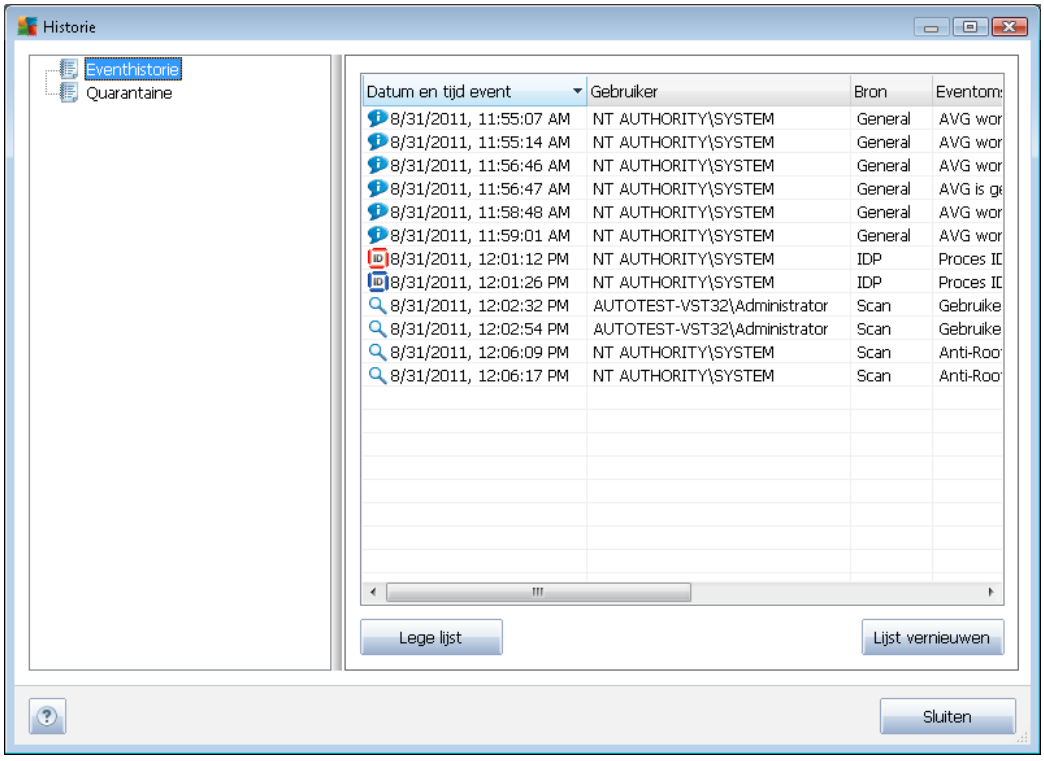
U kunt tijdens het plannen van een update specifieke parameters instellen voor beide updateniveaus:

- Schema definitie-updates

- Updateschema programma

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

12. Eventhistorie



U kunt het dialoogvenster ***Historie*** openen in het menu ***Historie / Logboek eventhistorie***. In het dialoogvenster wordt een overzicht weergegeven van belangrijke gebeurtenissen die tijdens het uitvoeren van **AVG Anti-Virus 2012** zijn opgetreden. In het logboek ***Historie worden de volgende gebeurtenistypen vastgelegd:***

- Informatie over updates van de AVG-toepassing
- Informatie over het begin, het einde en het onderbreken van een scan (*waaronder automatisch uitgevoerde scans*)
- Informatie over gebeurtenissen die verband houden met virusdetectie (*door Resident Shield of tijdens het scannen*), waaronder de detectielocatie
- Andere belangrijke gebeurtenissen

Voor elke gebeurtenis worden de volgende gegevens vastgelegd:

- ***Datum en tijd event*** – In deze kolom wordt het exacte moment vermeld waarop de gebeurtenis plaatshad
- ***Gebruiker*** – In deze kolom wordt de naam vermeld van de gebruiker die was aangemeld op het moment waarop de gebeurtenis plaatshad
- ***Bron*** – In deze kolom wordt het onderdeel of het deel van het systeem vermeld dat de aanleiding vormde voor de gebeurtenis

- ***Beschrijving gebeurtenis*** – een korte samenvatting van wat er feitelijk gebeurde

Knoppen

- ***Lege lijst*** – Druk op deze knop als u alle vermeldingen uit de lijst wilt verwijderen
- ***Lijst vernieuwen*** – Druk op deze knop als u alle vermeldingen in de lijst wilt vernieuwen

13. Veelgestelde vragen en technische ondersteuning

Als u op problemen met betrekking tot de verkoop of op technische problemen met uw **AVG Anti-Virus 2012** -toepassing stuit, kunt u op verscheidene manieren naar hulp zoeken. U kunt kiezen uit de volgende mogelijkheden:

- ***Contact opnemen met de klantenondersteuning***: U kunt vanuit de AVG-toepassing contact opnemen met onze professionele klantenondersteuning. Selecteer het hoofdmenu-item ***Help / Help Online***, zodat het online contactformulier wordt weergegeven. U kunt via dit formulier contact opnemen met de AVG-klantenondersteuning. Deze is zeven dagen per week en 24 uur per dag bereikbaar. Uw licentienummer wordt automatisch ingevuld. Volg vervolgens de instructies op de webpagina.

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

- ***Problemen oplossen in het Help-bestand***: er is een nieuwe sectie met de naam ***Problemen oplossen*** beschikbaar in het Help-bestand in **AVG Anti-Virus 2012**. Deze sectie biedt een lijst met regelmatig voorkomende situaties waarin een gebruiker behoefte heeft aan professionele hulp met betrekking tot een technisch probleem. Selecteer de situatie die uw probleem het beste beschrijft en klik op de koppeling om gedetailleerde instructies weer te geven voor het oplossen van het probleem.

- ***Ondersteuningscentrum op de AVG-website***: het is ook mogelijk om op de website van AVG naar een oplossing voor uw probleem te zoeken (http://www.avg.com/). In de sectie

Help vindt u een gestructureerd overzicht van thematische groepen voor verkoopgebonden problemen en technische problemen.

- ***Veelgestelde vragen***: de AVG-website (http://www.avg.com/) omvat tevens een aparte, bijzonder gedetailleerde sectie met veelgestelde vragen. Deze sectie is toegankelijk via de menuoptie ***Help / FAQ***. Ook hier zijn alle vragen keurig gerangschikt op basis van verkoopgebonden, technische en virusgebonden categorieën.

- ***Info virussen en bedreigingen***: een aparte sectie van de AVG-website (http://www.avg.com/) heeft betrekking op virusgebonden problemen. Selecteer ***Help / Info virussen en bedreigingen*** in het menu als u een pagina wilt openen die een gestructureerd overzicht bevat van alle online bedreigingen. Daarnaast vindt u hier instructies voor het verwijderen van virussen en spyware en advies met betrekking tot hoe u beveiligd kunt blijven.

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