



AVG Internet Security 2011

Gebruikershandleiding

Documentrevisie 2011.21 (16.5.2011)

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 libzip2, copyright (c) 1996-2002 Julian R. Seward.



Inhoud

1. Inleiding	8
2. AVG installatievereisten	9
2.1 Ondersteunde besturingssystemen	9
2.2 Minimale en aanbevolen hardwarevereisten	9
3. AVG installatieopties	10
4. AVG installatieprocedure	11
4.1 Welkom	11
4.2 Uw AVG-licentie activeren	12
4.3 Type installatie selecteren	13
4.4 Aangepaste opties	14
4.5 De AVG Werkbalk Beveiliging installeren	15
4.6 Installatievoortgang	16
4.7 Installatie voltooid	16
5. Na de installatie	18
5.1 Productregistratie	18
5.2 Toegang tot gebruikersinterface	18
5.3 Volledige computerscan	18
5.4 De EICAR-test	18
5.5 AVG standaardconfiguratie	19
6. AVG gebruikersinterface	20
6.1 Systeemmenu	21
6.1.1 Bestand	21
6.1.2 Onderdelen	21
6.1.3 Historie	21
6.1.4 Extra	21
6.1.5 Help	21
6.2 Info Beveiligingsstatus	24
6.3 Snelkoppelingen	25
6.4 Overzicht van onderdelen	25
6.5 Statistieken	27
6.6 Systeemvakpictogram	27
6.7 AVG gadget	28



7. AVG onderdelen	31
7.1 Antivirus	31
7.1.1 Antivirus - basisbegrippen	31
7.1.2 Antivirus interface	31
7.2 Antispyware	32
7.2.1 Antispyware – basisbegrippen	32
7.2.2 Antispyware interface	32
7.3 Antispam	34
7.3.1 Antispam principes	34
7.3.2 Antispam interface	34
7.4 Firewall	35
7.4.1 Firewallprincipes	35
7.4.2 Firewallprofielen	35
7.4.3 Firewallinterface	35
7.5 LinkScanner	39
7.5.1 LinkScanner principes	39
7.5.2 Interface LinkScanner	39
7.5.3 Search-Shield	39
7.5.4 Surf-Shield	39
7.6 Resident Shield	43
7.6.1 Resident Shield principes	43
7.6.2 Resident Shield interface	43
7.6.3 Resident Shield detectie	43
7.7 Veiligheid voor het gezin	48
7.8 AVG LiveKive	48
7.9 E-mailscanner	48
7.9.1 E-mailscanner principes	48
7.9.2 E-mailscanner interface	48
7.9.3 E-mailscanner detectie	48
7.10 Updatebeheer	52
7.10.1 Updatebeheer principes	52
7.10.2 Updatebeheer interface	52
7.11 Licentie	54
7.12 Extern beheer	55
7.13 Online Shield	56
7.13.1 Online Shield principes	56
7.13.2 Online Shield interface	56



7.13.3 Online Shield detectie	56
7.14 Antirootkit	59
7.14.1 Antirootkit principes	59
7.14.2 Antirootkit interface	59
7.15 Systeemprogramma's	61
7.15.1 Processen	61
7.15.2 Netwerkverbindingen	61
7.15.3 Autostart	61
7.15.4 Browserextensies	61
7.15.5 LSP-viewer	61
7.16 PC Analyzer	66
7.17 ID Protection	68
7.17.1 ID Protection principes	68
7.17.2 ID Protection interface	68
7.18 Werkbalk Beveiliging	70
8. AVG Werkbalk Beveiliging	72
8.1 Interface van de AVG Werkbalk Beveiliging	72
8.1.1 Knop AVG-logo	72
8.1.2 Zoekvak van AVG Secure Search (powered by Google)	72
8.1.3 Paginastatus	72
8.1.4 AVG Nieuws	72
8.1.5 Nieuws	72
8.1.6 Historie wissen	72
8.1.7 E-mailmelding	72
8.1.8 Weerinfo	72
8.1.9 Facebook	72
8.2 AVG Werkbalk Beveiliging opties	79
8.2.1 Tabblad Algemeen	79
8.2.2 Tabblad Handige knoppen	79
8.2.3 Tabblad Beveiliging	79
8.2.4 Tabblad Geavanceerde opties	79
9. AVG Geavanceerde instellingen	84
9.1 Weergave	84
9.2 Geluiden	86
9.3 Status negeren	88
9.4 Identity Protection	89
9.4.1 Identity Protection instellingen	89



9.4.2 Lijst Toegestaan	89
9.5 Quarantaine	93
9.6 PUP-uitzonderingen	93
9.7 Antispam	95
9.7.1 Instellingen	95
9.7.2 Prestaties	95
9.7.3 RBL	95
9.7.4 Witte lijst	95
9.7.5 Zwarte lijst	95
9.7.6 Geavanceerde instellingen	95
9.8 Online Shield	107
9.8.1 Webbescherming	107
9.8.2 Expresberichten	107
9.9 LinkScanner	111
9.10 Scans	112
9.10.1 De hele computer scannen	112
9.10.2 Shell-extensiescan	112
9.10.3 Bepaalde mappen of bestanden scannen	112
9.10.4 Scan van verwisselbaar apparaat	112
9.11 Schema's	118
9.11.1 Geplande scan	118
9.11.2 Updateschema virusdatabase	118
9.11.3 Updateschema programma	118
9.11.4 Antispam updateschema	118
9.12 E-mailscanner	131
9.12.1 Certificatie	131
9.12.2 Mailfiltering	131
9.12.3 Servers	131
9.13 Resident Shield	140
9.13.1 Geavanceerde instellingen	140
9.13.2 Uitgesloten onderdelen	140
9.14 Cacheserver	144
9.15 Antirookit	145
9.16 Update	146
9.16.1 Proxy	146
9.16.2 Inbellen	146
9.16.3 URL	146
9.16.4 Beheer	146



9.17 AVG-bescherming tijdelijk uitschakelen	153
9.18 Programma voor productverbetering	153
10. Firewallinstellingen	156
10.1 Algemeen	156
10.2 Beveiliging	157
10.3 Profielen van gebieden en adapters	158
10.4 IDS	159
10.5 Logboeken	161
10.6 Profielen	163
11. AVG scannen	165
11.1 Scaninterface	165
11.2 Vooraf ingestelde scans	166
11.2.1 De hele computer scannen	166
11.2.2 Bepaalde mappen of bestanden scannen	166
11.2.3 Antirootkitscan	166
11.3 Scannen in Windows Verkenner	176
11.4 Scannen vanaf opdrachtregel	177
11.4.1 CMD-scanparameters	177
11.5 Scans plannen	179
11.5.1 Schema-instellingen	179
11.5.2 Hoe er gescand moet worden	179
11.5.3 Wat er gescand moet worden	179
11.6 Overzicht scanresultaten	189
11.7 Details scanresultaten	190
11.7.1 Tabblad Overzicht resultaten	190
11.7.2 Tabblad Infecties	190
11.7.3 Tabblad Spyware	190
11.7.4 Tabblad Waarschuwingen	190
11.7.5 Tabblad Rootkits	190
11.7.6 Tabblad Informatie	190
11.8 Quarantaine	198
12. AVG Updates	200
12.1 Updateniveaus	200
12.2 Soorten updates	200
12.3 Updateprocedure	200



13. Eventhistorie	202
14. Veelgestelde vragen en technische ondersteuning	204



1. Inleiding

Deze gebruikershandleiding bevat uitgebreide informatie over **AVG Internet Security 2011**.

Gefeliciteerd met uw aankoop van AVG Internet Security 2011!

AVG Internet Security 2011 is één van een reeks onderscheiden AVG-producten die zijn ontwikkeld om uw gemoedsrust te bevorderen en uw pc volledig te beschermen. Net als alle andere AVG-producten is **AVG Internet Security 2011** volledig opnieuw vormgegeven, vanaf het fundament, om de bekende en geroemde beveiliging van AVG aan te kunnen bieden op een nieuwe, meer gebruiksvriendelijke en efficiëntere manier. Uw nieuwe **AVG Internet Security 2011**-product heeft een gestroomlijnde interface gecombineerd met agressievere en snellere scanprocedures. Om het u gemakkelijk te maken zijn meer beveiligingsfuncties geautomatiseerd, en zijn nieuwe, 'intelligente' gebruikersopties toegevoegd, zodat u onze beveiligingsfuncties aan uw wensen kunt aanpassen. Geen compromissen meer tussen veiligheid en gemak!

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

Aanbod van alle AVG-producten

- Bescherming die aansluit op de manier waarop u internet gebruikt: bankieren en winkelen, surfen en zoeken, chatten en e-mailen of bestanden downloaden en sociaal netwerken – AVG heeft een beveiligingsproduct voor u
- Bescherming zonder gezeur, waarop meer dan 110 miljoen mensen wereldwijd vertrouwen, gevoed door een wereldwijd netwerk van uiterst deskundige wetenschappers
- Bescherming met deskundige ondersteuning, 24 uur per etmaal



2. AVG installatievereisten

2.1. Ondersteunde besturingssystemen

AVG Internet Security 2011 is ontworpen om werkstations met de volgende besturingssystemen te beschermen:

- Windows XP Home Edition SP2
- Windows XP Professional SP2
- Windows XP Professional x64 Edition SP1
- Windows Vista (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 `%main_product_name_in_text%` op deze besturingssystemen installeren, maar dan zonder het onderdeel IDP.

2.2. Minimale en aanbevolen hardwarevereisten

Minimale hardwarevereisten voor **AVG Internet Security 2011**:

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

Aanbevolen hardwarevereisten voor **AVG Internet Security 2011**:

- Intel Pentium CPU 1,8 GHz
- 512 MB RAM-geheugen
- 1400 MB vrije schijfruimte (voor de installatie)



3. AVG installatieopties

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

Voordat u AVG installeert, raden wij u nadrukkelijk aan de website van AVG(<http://www.avg.com/>) te bezoeken om na te gaan of er een nieuw installatiebestand is. Zo bent u er zeker van dat u de meest recente versie van AVG Internet Security 2011 installeert.

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



4. AVG installatieprocedure

Als u **AVG Internet Security 2011** op uw computer wilt installeren, moet u over het meest recente installatiebestand beschikken. U kunt het installatiebestand gebruiken dat op de cd staat die onderdeel uitmaakt van de editie in de doos, maar dat bestand kan verouderd zijn. We raden u daarom aan het nieuwste installatiebestand online op te vragen. U kunt dit downloaden van de AVG-website (<http://www.avg.com/>), vanaf de pagina [Ondersteuningscentrum / Downloads](#).

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

4.1. Welkom

Bij de start van de installatieprocedure wordt het venster **Welkom** weergegeven. In dat dialoogvenster kiest u de taal die bij de installatie moet worden gebruikt en de standaardtaal voor de AVG-gebruikersinterface. In het bovenste deel van het venster staat een vervolkeuzelijst met de talen waaruit u kunt kiezen:



Let op: u selecteert hier alleen een taal voor de installatieprocedure. De taal die u selecteert, zal als standaardtaal worden geïnstalleerd voor de gebruikersinterface van AVG, samen met Engels, dat automatisch wordt geïnstalleerd. Als u nog meer talen voor de gebruikersinterface wilt installeren, geeft u die op in het installatiedialoogvenster [Aangepaste opties](#).

In dit dialoogvenster staat de volledige tekst van de AVG licentieverklaring. 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.



4.2. Uw AVG-licentie activeren

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

Het verkoopnummer vindt u op de cd-verpakking in de doos met **AVG Internet Security 2011**. Het licentienummer staat in de bevestiging die u via e-mail hebt ontvangen na aankoop van **AVG Internet Security 2011** 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.

Installatieprogramma AVG-software

AVG Uw licentie activeren

Licentienummer:

Voorbeeld: 9FULL-NSDRS-KUL4L-UKSFR-L96M9-B2ALT-XWMX3

Als u de software voor AVG 2011 online hebt aangeschaft, hebt u uw licentienummer per e-mail ontvangen. We raden u aan het nummer uit de e-mail te knippen en in dit scherm te plakken, om fouten bij het intypen te voorkomen.

Als u de software in de winkel hebt gekocht, staat het licentienummer vermeld op de registratiekaart die u in het pakket vindt. Zorg ervoor dat u het nummer correct kopieert.

≤ Terug **Volgende ≥** Annuleren

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

4.3. Type installatie selecteren



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

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

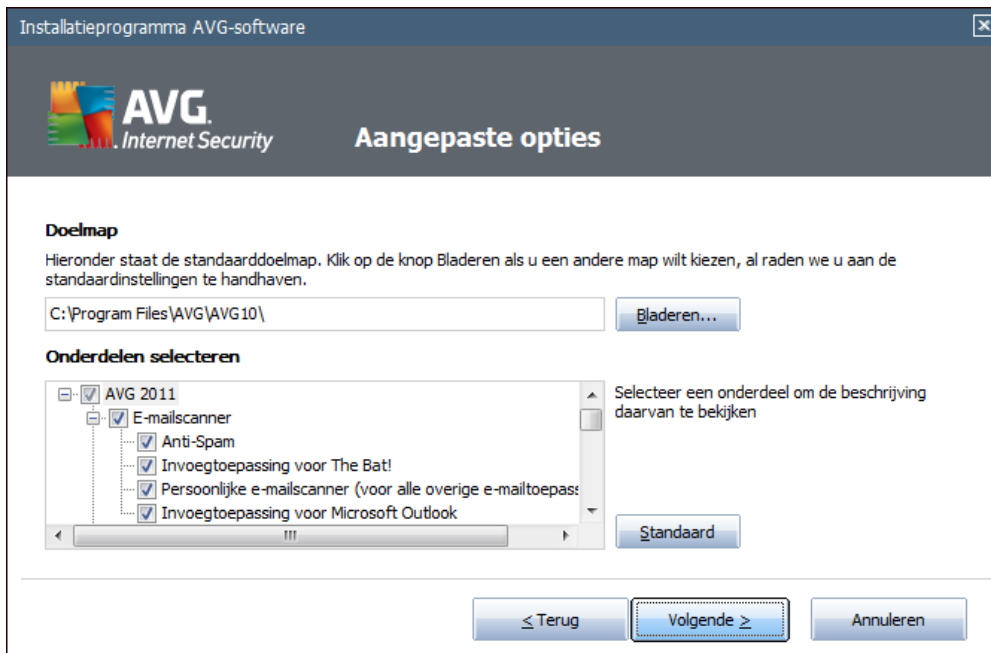
Een aangepaste installatie is alleen aanbevolen voor ervaren gebruikers die een goede reden hebben om AVG te installeren met afwijkende instellingen, bijvoorbeeld om te voldoen aan specifieke systeemvereisten. Als u deze optie hebt geselecteerd, klikt u op de knop **Volgende** om naar het dialoogvenster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

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 Internet Security 2011**, i.e. [scannen](#) en [updates](#).



4.4. 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 Internet Security 2011** wilt installeren. Standaard wordt AVG 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

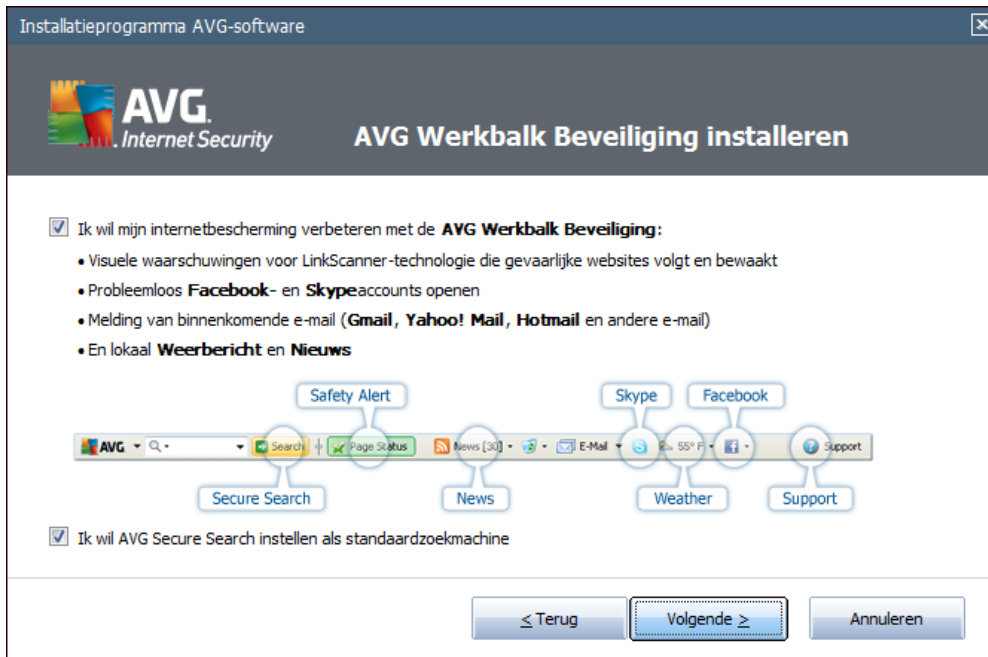
In het dialoogvenster **Onderdelen selecteren** staat een overzicht van alle onderdelen van **AVG Internet Security 2011** die kunnen worden geïnstalleerd. Als de standaardinstellingen niet voldoen, kunt u onderdelen toevoegen of verwijderen.

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.

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

4.5. 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, en biedt een 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.



4.6. Installatievoortgang

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



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

4.7. Installatie voltooid





Het dialoogvenster **Installatie voltooid** vormt de bevestiging van het feit dat **AVG Internet Security 2011** is geïnstalleerd en geconfigureerd.

We verzoeken u in dit dialoogvenster uw contactgegevens aan ons door te geven, zodat we u informatie en nieuws met betrekking tot uw product kunnen toezenden. Onder het registratieformulier staan de volgende twee opties:

- **Ja, houd mij op de hoogte van beveiligingsnieuws en stuur me speciale aanbiedingen voor AVG 2011 via e-mail** – met een vinkje in dit selectievakje geeft u aan dat u op de hoogte wilt blijven van de ontwikkelingen op het gebied van internetbeveiliging, en graag informatie wilt ontvangen over speciale aanbiedingen, verbeteringen, upgrades, enz. voor producten van AVG.
- **Ik ga akkoord met deelname aan het AVG 2011-programma voor internetveiligheid en het productverbeteringsprogramma...** – met een vinkje in dit selectievakje geeft u aan dat u wilt deelnemen aan het productverbeteringsprogramma (zie [AVG Geavanceerde instellingen / Productverbeteringsprogramma](#) voor meer informatie), waarmee anoniem gegevens worden verzameld over gedetecteerde bedreigingen om de algehele veiligheid op internet te vergroten.

Een herstart van de computer is vereist voor het voltooien van de installatie: maak een keuze voor **Nu herstarten**, of uitstel van een herstart – **Later herstarten**.

Opmerking: als u een zakelijke AVG-licentie hebt en er eerder voor hebt gekozen om *Extern beheer te installeren* (zie [Aangepaste opties](#)), wordt het dialoogvenster bij een voltooide installatie als volgt weergegeven:

*U dient AVG-Datacentergegevens op te geven – voer de verbindingstring 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**. Raadpleeg de gebruikershandleiding voor de AVG Business Edition voor meer informatie over AVG Extern beheer; u kunt die handleiding downloaden van de website van AVG (<http://www.avg.com/>).*



5. Na de installatie

5.1. Productregistratie

Registreer na het voltooien van de installatie van **AVG Internet Security 2011** uw product online op de website van AVG (<http://www.avg.com/>), pagina **Registratie** (*Volg de instructies op de pagina*). Na de registratie krijgt u volledige toegang tot uw gebruikersaccount bij AVG, de AVG Update nieuwsbrief en andere services die alleen beschikbaar zijn voor geregistreerde gebruikers.

5.2. Toegang tot gebruikersinterface

U kunt de [AVG gebruikersinterface](#) op meerdere manieren openen:

- 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 2011/AVG Gebruikersinterface**
- van de [AVG werkbalk Beveiliging](#) met de optie **AVG starten**

5.3. Volledige computerscan

Het risico bestaat dat er een computervirus naar uw computer is overgebracht voordat u **AVG Internet Security 2011** 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](#).

5.4. De EICAR-test

Als u zeker wilt weten of **AVG Internet Security 2011** 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](http://www.eicar.com) en sla het op naar uw lokale vaste schijf. Het onderdeel [Online shield](#) geeft onmiddellijk een waarschuwing weer nadat u de download van het testbestand hebt bevestigd. Deze waarschuwing toont aan dat AVG goed op uw computer is geïnstalleerd.



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

5.5. AVG standaardconfiguratie

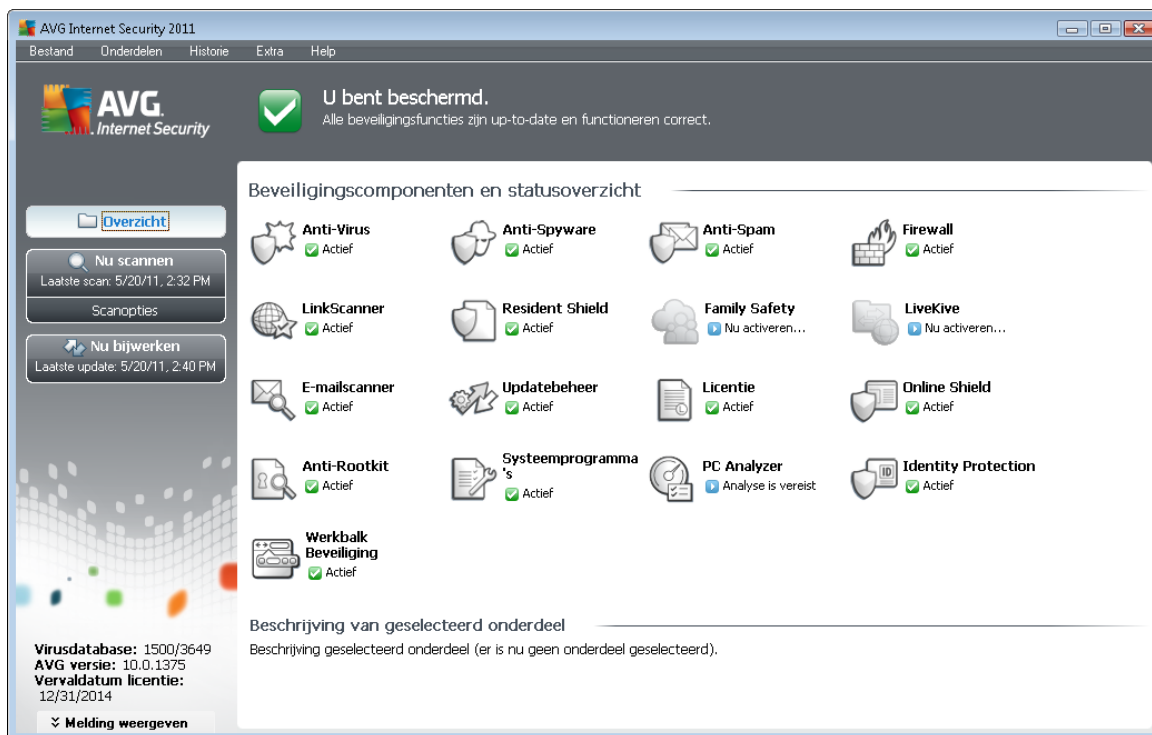
De standaardconfiguratie (*dat wil zeggen de manier waarop de toepassing functioneert meteen na installatie*) van **AVG Internet Security 2011** is het werk van de leverancier van de software: alle onderdelen en functies zijn zo ingesteld dat de toepassing optimaal presteert.

***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.

6. AVG gebruikersinterface

AVG Internet Security 2011 wordt geopend met het hoofdvenster:



Het hoofdvenster is onderverdeeld in een aantal secties:

- **Systeemmenu** (de menubalk boven in het venster), het standaardmenu voor het navigeren naar alle onderdelen, services en functies van AVG - [details >>](#)
- **Info Beveiligingsstatus** (bovenste deel van het venster), informatie over de huidige status van AVG - [details >>](#)
- **Snelkoppelingen** (linker deelvenster), koppelingen naar de belangrijkste en meest gebruikte AVG-functies - [details >>](#)
- **Onderdelenoverzicht** (centrale deel van het venster), overzicht van alle geïnstalleerde onderdelen van AVG - [details >>](#)
- **Statistieken** (links onder in het venster), alle statistische gegevens over de uitvoering van de programma's - [details >>](#)
- **Pictogram systeemvak** (rechts onder in het bureaublad van Windows, in het systeemvak), indicatie van de huidige status van AVG - [details >>](#)
- **AVG gadget** (Windows Sidebar, ondersteund in Windows Vista/7), snelle toegang tot scans en updates van AVG - [details >>](#)



6.1. 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 Internet Security 2011** geplaatst. Met behulp van het systeemmenu heeft u toegang tot de AVG onderdelen, functies en services.

Het systeemmenu is onderverdeeld in vijf secties:

6.1.1. Bestand

- **Afsluiten** - afsluiten van de **AVG Internet Security 2011**-gebruikersinterface. De AVG toepassing zal echter op de achtergrond actief blijven en uw computer is nog steeds beschermd!

6.1.2. 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** biedt uw computer bescherming tegen virussen die uw computer proberen binnen te dringen – [details >>](#)
- **Anti-Spyware** beschermt uw computer tegen spyware en adware – [details >>](#)
- **Anti-Spam** controleert alle binnenkomende e-mailberichten en markeert ongewenste e-mails als SPAM – [details >>](#)
- **Firewall** beheert hoe uw computer gegevens uitwisselt met andere computers op internet of in het lokale netwerk – [details >>](#)
- **LinkScanner** controleert zoekresultaten die in uw browser worden weergegeven – [details >>](#)
- **E-mailscanner** controleert alle binnenkomende en uitgaande e-mail op virussen – [details >>](#)
- **Veiligheid voor het gezin** bewaking van de online activiteiten van kinderen en bescherming tegen ongepaste inhoud van websites – [details >>](#)
- **LiveKive** automatische back-up van gegevens online – [details >>](#)
- **Resident Shield** wordt op de achtergrond uitgevoerd en scant bestanden als ze worden gekopieerd, geopend of opgeslagen – [details >>](#)
- **Updatebeheer** beheert alle AVG updates – [details >>](#)
- **Licentie** bevat informatie over het licentienummer, -type en de vervaldatum – [details >>](#)



- **Online Shield** scant alle gegevens die door een webbrowser worden gedownload – [details >>](#)
- **Anti-Rootkit** detecteert programma's en technologieën die proberen malware te camoufleren – [details >>](#)
- **Systeemprogramma's** bieden een gedetailleerd overzicht van de AVG-omgeving en informatie over het besturingssysteem – [details >>](#)
- **PC Analyzer** Verzorgt informatie over de status van de computer – [details >>](#)
- **Identity Protection** anti-malware-onderdeel gericht op het voorkomen van diefstal van waardevolle persoonlijke digitale gegevens – [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

6.1.3. Historie

- **Scanresultaten** - de AVG testinterface wordt geopend, in het bijzonder het dialoogvenster [Overzicht scanresultaten](#)
- **Resident Shield detectie** – er wordt een overzicht geopend met bedreigingen die zijn gedetecteerd door [Resident Shield](#)
- **E-mailscannerdetectie** - er wordt een overzicht geopend met bijlagen bij e-mailberichten die als gevaarlijk zijn gedetecteerd door het onderdeel [E-mailscanner](#)
- **Online Shield resultaten** – er wordt een overzicht geopend met bedreigingen die zijn gedetecteerd door [Online Shield](#)
- **Quarantaine** - de interface van de [Quarantaine](#) wordt geopend, waar AVG alle gedetecteerde infecties opslaat die om de een of andere reden niet automatisch kunnen worden hersteld. In de quarantaine worden de geïnfecteerde bestanden geïsoleerd, zodat uw computer veilig blijft, terwijl het opslaan van de bestanden eventueel herstel van de bestanden in de toekomst mogelijk maakt
- **Logboek Eventhistorie** – het dialoogvenster wordt geopend met de geschiedenis van alle vastgelegde **AVG Internet Security 2011 acties van**
- **Firewall** – het dialoogvenster Firewall-instellingen wordt geopend, en op het tabblad [Logboeken](#) staat een gedetailleerd overzicht van alle acties die Firewall heeft ondernomen

6.1.4. 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 enkel bestand selecteren dat u wilt scannen.
- **Update** – automatisch de updateprocedure starten van **AVG Internet Security 2011**.
- **Bijwerken vanuit directory** – de updateprocedure wordt gestart aan de hand van updatebestanden in een bepaalde map op de lokale vaste schijf. Deze optie wordt echter alleen aanbevolen als noodprocedure, bijvoorbeeld onder omstandigheden waarbij er geen verbinding is met internet (*uw computer is bijvoorbeeld geïnfecteerd en afgesloten van internet; uw computer is aangesloten op een netwerk zonder verbinding met internet, enz.*). Selecteer in het venster dat wordt geopend, de map waarin u eerder het updatebestand hebt opgeslagen, en start de updateprocedure.
- **Geavanceerde instellingen** – het dialoogvenster **AVG Geavanceerde instellingen** wordt geopend waarin u de configuratie van **AVG Internet Security 2011** kunt wijzigen. Over het algemeen is het raadzaam de standaardinstellingen aan te houden, zoals die zijn ingesteld door de leverancier van de software.
- **Firewall-instellingen** – er wordt een standalone dialoogvenster geopend voor geavanceerde configuratie van het onderdeel **Firewall**.

6.1.5. Help

- **Inhoud** – de Help-bestanden van AVG worden geopend
- **Online Help** - de website van AVG (<http://www.avg.com/>) wordt geopend op de pagina voor klantenservice
- **Uw AVG-web** - de website van AVG (<http://www.avg.com/>) openen
- **Over virussen & bedreigingen** – de online **Virusencyclopedie** wordt geopend, waarin u gedetailleerde informatie kunt zoeken over bekende virussen
- **Opnieuw activeren** - het dialoogvenster **AVG activeren** wordt geopend met de gegevens die u heeft opgegeven in het dialoogvenster **AVG aanpassen** van de **installatieprocedure**. In dit dialoogvenster kunt u uw licentienummer invoeren ter vervanging van ofwel het verkoopnummer (*het nummer waarmee u AVG heeft geïnstalleerd*), ofwel het oude licentienummer (*bijvoorbeeld bij het upgraden naar een nieuw product van AVG*).
- **Nu registreren** - verbinding maken met de registratiepagina van de website van AVG (<http://www.avg.com/>). Voer uw registratiegegevens in; alleen klanten die hun AVG product registreren komen in aanmerking voor gratis technische ondersteuning.

Opmerking: Als u de proefversie van **AVG Internet Security 2011** 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 Internet Security 2011** hebt geïnstalleerd met een verkoopnummer, worden deze items weergegeven als **Registreren** en **Activeren**. Zie voor meer informatie het gedeelte **Licentie** in deze documentatie.



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

6.2. Info Beveiligingsstatus

De sectie **Info Beveiligingsstatus** bevindt zich in het bovenste deel van het hoofdvenster van AVG. In deze sectie staat altijd informatie over de huidige beveiligingsstatus van **AVG Internet Security 2011**. Hieronder volgt een overzicht van de pictogrammen die in deze sectie kunnen worden weergegeven, en hun betekenis:



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



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

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



Een rood pictogram geeft aan dat er een kritieke situatie is! Eén of meer onderdelen functioneren niet correct en AVG kan uw computer niet beschermen. Besteed onmiddellijk aandacht aan het probleem en probeer het te verhelpen. Als het u niet lukt de fout zelf te herstellen, neem dan contact op met het team van de [Technische ondersteuning van AVG](#).

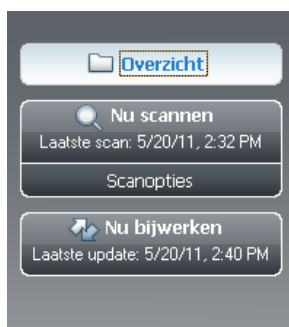
Als de instellingen van AVG niet zijn ingesteld voor optimaal presteren, wordt een nieuwe knop met de naam Repareren (of Alles repareren als het probleem meer dan één onderdeel betreft) weergegeven naast de informatie over de beveiligingsstatus. Klik op die knop om een automatisch proces voor programmacontrole en -configuratie te starten. Dat is een eenvoudige manier om AVG in te stellen op optimaal presteren en de hoogste graad van veiligheid te bereiken!

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

Opmerking: u kunt ook, wanneer u maar wilt, statusinformatie over AVG opvragen via het [systeemvak pictogram](#).

6.3. Snelkoppelingen

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



- **Overzicht** – klik op deze snelkoppeling om vanuit een geopend dialoogvenster van AVG terug te keren naar het Overzicht van alle geïnstalleerde onderdelen – zie het hoofdstuk [Overzicht van onderdelen >>](#)
- **Nu scannen** – standaard biedt de knop (*scantype, datum laatste scanstart*) informatie over de laatste gestarte scan. U kunt met de opdracht **Nu scannen** diezelfde scan opnieuw starten, maar u kunt ook met de koppeling **Scanopties** de scaninterface van AVG openen, waarin u scans kunt uitvoeren, scans kunt plannen, of de parameters voor scans kunt wijzigen – zie het hoofdstuk [AVG scannen >>](#)
- **Nu bijwerken** – de koppeling biedt de datum van de laatste keer dat het updateproces is gestart. Klik op de knop om de update-interface te openen en het updateproces direct uit te voeren – zie het hoofdstuk [AVG Updates >>](#)

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

6.4. Overzicht van onderdelen

De sectie **Overzicht van onderdelen** staat in het middelste gedeelte van de [AVG gebruikersinterface](#). De sectie is onderverdeeld in twee gedeeltes:

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

De sectie **Overzicht van onderdelen** in **AVG Internet Security 2011** bevat informatie over de



volgende onderdelen:

- **Anti-Virus** biedt uw computer bescherming tegen virussen die uw computer proberen binnen te dringen – [details >>](#)
- **Anti-Spyware** beschermt uw computer tegen spyware en adware – [details >>](#)
- **Anti-Spam** controleert alle binnenkomende e-mailberichten en markeert ongewenste e-mails als SPAM – [details >>](#)
- **Firewall** beheert hoe uw computer gegevens uitwisselt met andere computers op internet of in het lokale netwerk – [details >>](#)
- **LinkScanner** controleert zoekresultaten die in uw browser worden weergegeven – [details >>](#)
- **E-mailscanner** controleert alle binnenkomende en uitgaande e-mail op virussen – [details >>](#)
- **Resident Shield** wordt op de achtergrond uitgevoerd en scant bestanden als ze worden gekopieerd, geopend of opgeslagen – [details >>](#)
- **Veiligheid voor het gezin** bewaking van de online activiteiten van kinderen en bescherming tegen ongepaste inhoud van websites – [details >>](#)
- **LiveKive** automatische back-up van gegevens online – [details >>](#)
- **Updatebeheer** beheert alle AVG updates – [details >>](#)
- **Licentie** bevat informatie over het licentienummer, -type en de vervaldatum – [details >>](#)
- **Online Shield** scant alle gegevens die door een webbrowser worden gedownload – [details >>](#)
- **Anti-Rootkit** detecteert programma's en technologieën die proberen malware te camoufleren – [details >>](#)
- **Systeemprogramma's** bieden een gedetailleerd overzicht van de AVG-omgeving en informatie over het besturingssysteem – [details >>](#)
- **PC Analyzer** Verzorgt informatie over de status van de computer – [details >>](#)
- **Identity Protection** anti-malware-onderdeel gericht op het voorkomen van diefstal van waardevolle persoonlijke digitale gegevens – [details >>](#)
- **Werkbalk Beveiliging** [AVG-functionaliteit direct beschikbaar vanuit de webbrowser](#)
- **Extern beheer** wordt alleen weergegeven in AVG Business Editions als u tijdens het [installatieproces](#) hebt aangegeven dat het onderdeel moest worden geïnstalleerd



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

Klik met de rechtermuisknop op een pictogram van een onderdeel om een snelmenu te openen: behalve het openen van de grafische interface van het onderdeel kunt u ook **Onderdeelstatus negeren** selecteren. Selecteer deze optie om aan te geven dat u zich bewust bent van de [foutstatus van het onderdeel](#), maar dat u om een bepaalde reden uw AVG ongewijzigd wilt laten en niet wilt worden gewaarschuwd door het [systeemvakpictogram](#).

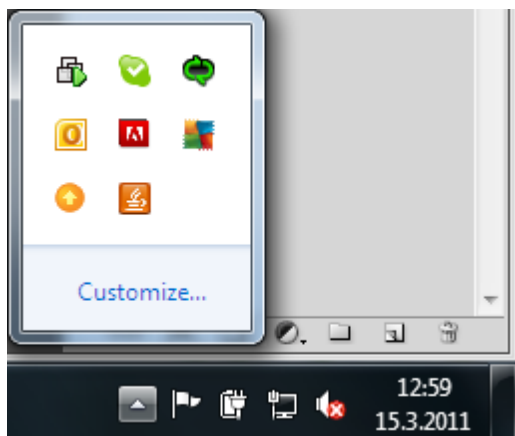
6.5. Statistieken



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

- **Virusdatabase** – informatie over de huidige geïnstalleerde versie van de virusdatabase
- **AVG-versie** – informatie over de geïnstalleerde AVG-versie (een nummer met de opmaak 10.0.xx, waarbij 10.0 de productversie is en xx voor het typenummer staat)
- **Vervaldatum licentie** – de vervaldatum van uw AVG-licentie

6.6. Systeemvakpictogram

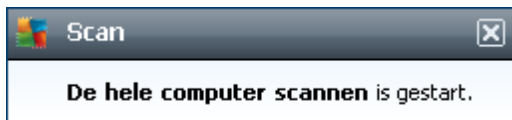
Het systeemvakpictogram (op de Taakbalk van Windows) geeft de huidige status van **AVG Internet Security 2011** aan. Het pictogram wordt steeds weergegeven in het systeemvak, ongeacht of het hoofdvenster van AVG is geopend of gesloten:



Als alle kleuren te zien zijn , geeft het **systeemvakpictogram** aan dat alle AVG-onderdelen actief zijn en geheel naar behoren werken. Het systeemvakpictogram van AVG kan ook worden weergegeven in vier kleuren als AVG een foutstatus heeft, maar u geheel op de hoogte bent van deze situatie en bewust hebt besloten [de onderdeelstatus te negeren](#). Een pictogram met een uitroepteken  duidt op een probleem (niet-actief onderdeel, foutstatus, enz.). Dubbelklik op het **systeemvakpictogram** om het hoofdvenster te openen en een onderdeel aan te passen.



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



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



- **AVG gebruikersinterface openen** – klik op de optie als u de [AVG gebruikersinterface](#)
- **Scans** -
- **Firewall** – het snelmenu openen met opties voor [Firewall](#)instellingen voor het wijzigen van de belangrijkste parameters: [Firewallstatus](#) (*Firewall ingeschakeld/Firewall uitgeschakeld/Noodmodus*) [Gamingmodus in-/uitschakelen](#) en [Firewallprofielen](#)
- **Voer PC Analyzer uit** – het programma [PC Analyzer](#) starten
- **Actieve scans** – deze optie wordt alleen weergegeven als op dat moment een scan wordt uitgevoerd. U kunt dan 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** – onmiddellijk starten van een [update](#)
- **Help** – het Helpbestand openen op de introductiepagina

6.7. 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 Internet Security 2011**, namelijk [scannen](#) en [updates](#):

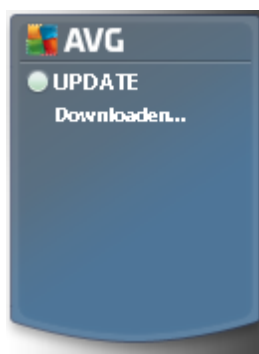



AVG gadget biedt de volgende opties voor snelle toegang:

- **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 standaarddialogvenster [Overzicht scanresultaten](#) voor meer informatie over de scanresultaten; u opent dat dialogvenster rechtstreeks vanaf de gadget met de optie **Details weergeven** (de desbetreffende scanresultaten staan bij **Sidebargadgets**).



- **Nu bijwerken** – als u op de koppeling **Nu bijwerken** klikt, wordt AVG Update direct vanuit de gadget gestart:



- **Twitter-koppeling**  – een nieuwe **AVG gadget** interface openen 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 van de licenties voor een AVG Business Edition*); de internetbrowser wordt geopend met de website **AVG SMB Community** in het sociale netwerk LinkedIn
- **PC Analyzer**  – 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 standaard webbrowser



7. AVG onderdelen

7.1. Antivirus

7.1.1. Antivirus - basisbegrippen

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

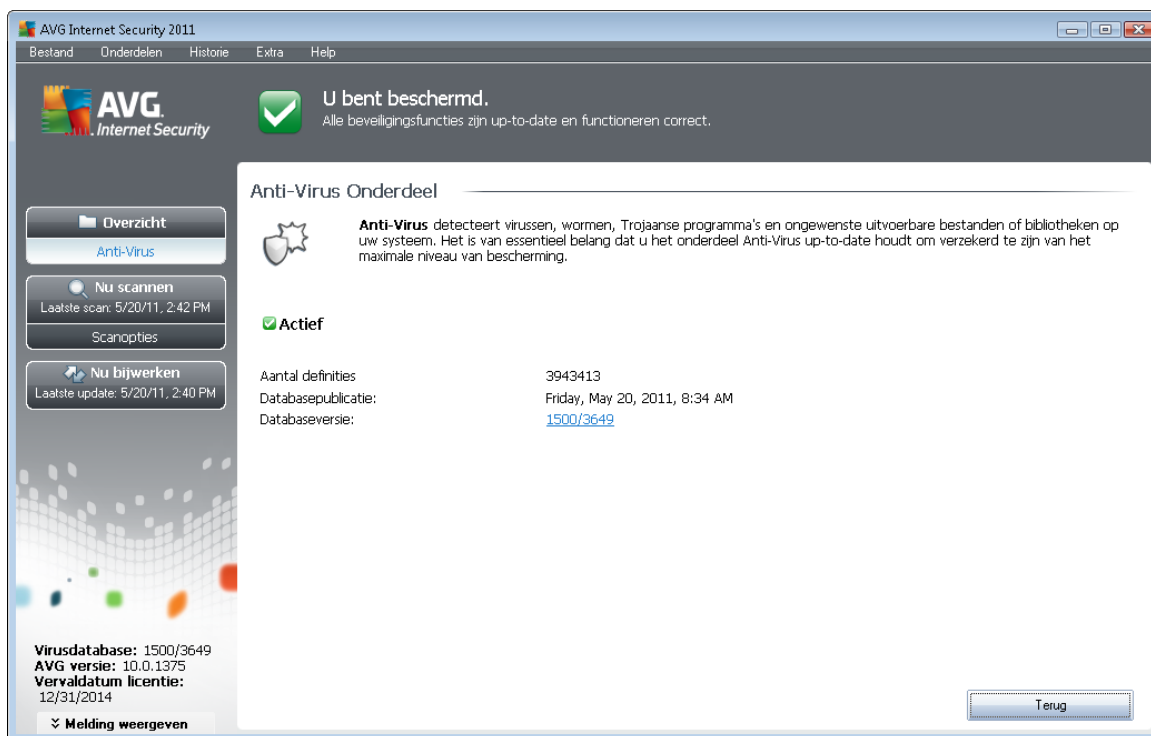
De belangrijkste functie van bescherming tegen virussen is het verhinderen van activiteit van bekende virussen!

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

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

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

7.1.2. Antivirus interface



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

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

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

7.2. Antispyware

7.2.1. Antispyware – basisbegrippen

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

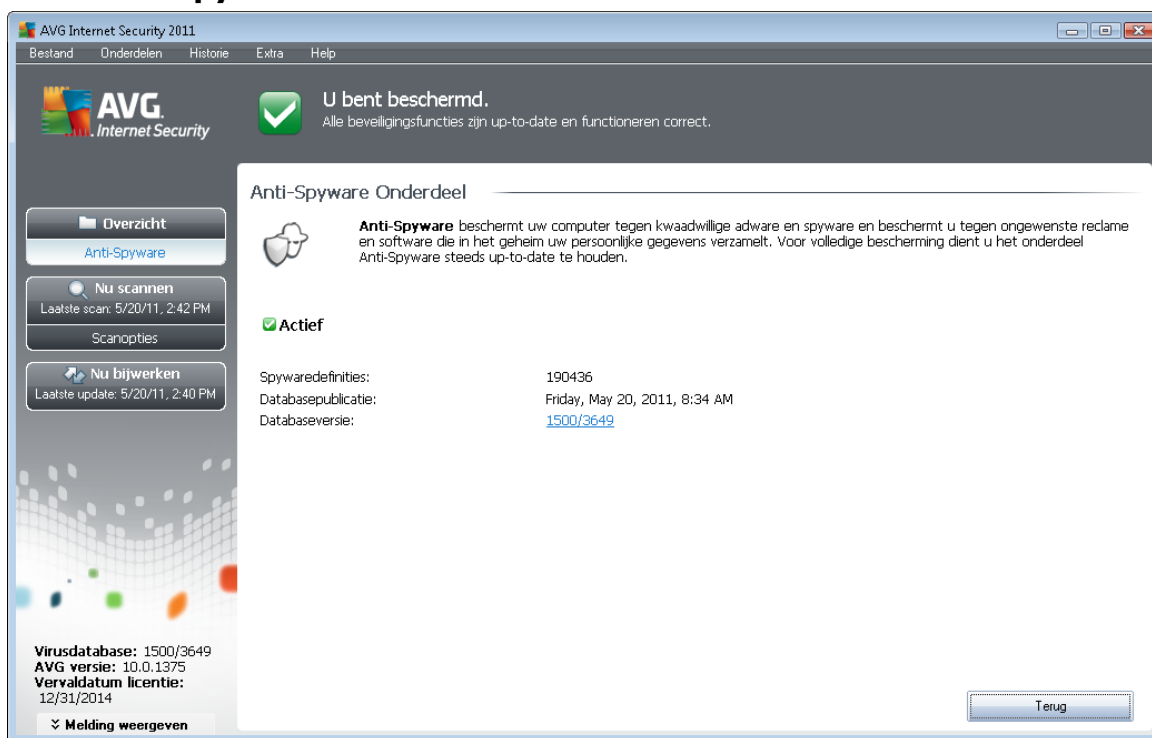


software.

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

Het is echter mogelijk dat uw computer reeds malware bevat op het moment dat u AVG op de computer installeert, of dat u **AVG Internet Security 2011** niet regelmatig hebt bijgewerkt met de recentste [database- en programma-updates](#). AVG is daarom voorzien van een scanfunctie waarmee u uw computer op malware/spyware kunt scannen. Die detecteert ook slapende en niet-actieve malware, dat wil zeggen malware die al wel is gedownload, maar nog niet is geactiveerd.

7.2.2. Antispyware interface



De interface van het onderdeel **Anti-Spyware** biedt een beknopt overzicht van de functionaliteit van het onderdeel, de huidige status, en enige cijfers over **Anti-Spyware**:

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



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

7.3. Antispam

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.

7.3.1. Antispam principes

AVG Anti-Spam controleert alle binnenkomende e-mailberichten en markeert ongewenste e-mails als spam. **AVG Anti-Spam** kan het onderwerp wijzigen van e-mail (*die is herkend als spam*) door er een speciale tekst aan toe te voegen. U kunt dan in uw e-mailclient de e-mails gemakkelijk filteren.

AVG Anti-Spam maakt gebruik van verschillende analysemethoden om elk e-mailbericht te verwerken. Dit biedt de best mogelijke bescherming tegen ongewenste e-mailberichten. **AVG Anti-Spam** maakt voor spamdetectie gebruik van een database die regelmatig wordt bijgewerkt. U kunt ook [RBL-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*).

7.3.2. Antispam interface

AVG Internet Security 2011

Bestand Onderdelen Historie Extra Help

AVG Internet Security

U bent beschermd. Alle beveiligingsfuncties zijn up-to-date en functioneren correct.

Anti-Spam Onderdeel

Het onderdeel **Anti-Spam** controleert alle binnenkomende e-mailberichten en markeert ongewenste e-mails als SPAM. Er worden meerdere analysemethoden toegepast die samen een zo groot mogelijke bescherming bieden.

Actief

Databasepublicatie:	Monday, November 03, 2008, 10:40 PM
Spamscatcherversie:	6.2.1
Aantal verwerkte e-mails:	1
Aantal spam-e-mails:	0
Aantal phishing-e-mails:	0

Selecteer [Extra / Geavanceerde instellingen...](#) in het systeemmenu voor meer gedetailleerde instellingen.

Anti-Spam-instellingen

Anti-Spam inschakelen

Wijzigingen opslaan Annuleren

Overzicht
Anti-Spam

Nu scannen
Laatste scan: 5/20/11, 2:42 PM
Scanopties

Nu bijwerken
Laatste update: 5/20/11, 2:40 PM

Virusdatabase: 1500/3649
AVG versie: 10.0.1375
Vervaldatum licentie: 12/31/2014
Melding weergeven

In het dialoogvenster van het onderdeel **Anti-Spam** staan een korte tekst met een beschrijving van de functionaliteit van het onderdeel, informatie over de huidige status en de volgende cijfers:



- **Databaseversie** – de datum en het tijdstip waarop de spamdatabase is bijgewerkt en gepubliceerd
- **Spamcatcherversie** – het nummer van de nieuwste versie van de anti-spam-engine
- **Aantal verwerkte e-mails** – opgave van het aantal gescande e-mailberichten vanaf het moment dat de anti-spam-engine voor het laatst is gestart
- **Aantal spam-e-mails** – opgave van het deel van alle gescande e-mails waarin spam is aangetroffen
- **Aantal phishing-e-mails** – opgave van het deel van alle gescande e-mails die zijn herkend als een poging tot phishing

In het dialoogvenster **Anti-spam** kunt u bovendien via het menu [Extra – Geavanceerde instellingen](#) geavanceerde instellingen opgeven. Het dialoogvenster waarin u een geavanceerde configuratie kunt opgeven voor alle onderdelen van **AVG Internet Security 2011** wordt dan geopend.

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

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

7.4. Firewall

Een firewall is een systeem dat een toegangsbeleid afdwingt tussen twee of meer netwerken door verkeer te blokkeren/toe te staan. Elke firewall heeft een reeks regels die het interne netwerk beschermen tegen aanvallen van buitenaf (meestal van internet) en die alle communicatie via elke netwerkpoort beheren. De communicatie wordt aan de hand van de gedefinieerde regels beoordeeld en dan toegestaan of verboden. Als de firewall inbreukpogingen herkent, wordt de poging geblokkeerd en krijgt de inbreker geen toegang tot de computer.

De firewall wordt geconfigureerd voor het toestaan of blokkeren van interne/externe communicatie (in beide richtingen, naar binnen en naar buiten) door opgegeven poorten, en voor opgegeven software. De Firewall kan bijvoorbeeld worden geconfigureerd om alleen gegevensstromen van internet (zowel binnenkomend als uitgaand) toe te staan via Microsoft Explorer. Elke poging om internetgegevens te verzenden of ontvangen via een andere browser zou dan worden geblokkeerd.

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

Aanbeveling: over het algemeen is het niet raadzaam om meer dan één firewall op een individuele computer te gebruiken. De computer wordt niet beter beveiligd als u meer firewalls installeert. Het is waarschijnlijker dat er conflicten tussen deze twee programma's optreden. Daarom raden we u aan slechts één firewall op uw computer te gebruiken en alle andere firewalls te deactiveren om zo het



risico op mogelijke conflicten en hiermee verbonden problemen te voorkomen.

7.4.1. Firewallprincipes

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

Opmerking: AVG Firewall is niet bedoeld voor serverplatforms!

Wat AVG Firewall kan doen:

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

7.4.2. Firewallprofielen

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

Beschikbare profielen

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



- **Aangepaste profielen:**

- **Rechtstreeks verbonden met internet** – geschikt voor gewone bureaucomputers thuis die rechtstreeks verbinding maken met internet, en voor notebooks die verbinding maken met internet buiten het veilige bedrijfsnetwerk. Selecteer deze optie als u vanuit thuis verbinding maakt, of als u werkt in een klein bedrijfsnetwerk zonder echt centraal beheer. Selecteer bovendien deze optie als u op reis bent en verbinding maakt met uw notebook vanaf verschillende onbekende en mogelijk gevaarlijke plekken (*internetcafé, hotelkamer, enzovoort*). Er worden strengere regels gecreëerd, omdat er wordt aangenomen dat deze computers verder geen bescherming hebben en dus zo goed mogelijk beschermd moeten worden.
- **Computer in een domein** – geschikt voor computers in een lokaal netwerk, bijvoorbeeld het netwerk van een school of een bedrijfsnetwerk. Er wordt van uitgegaan dat het netwerk wordt beveiligd met aanvullende maatregelen, zodat een minder hoog beveiligingsniveau vereist is dan bij standalone computers.
- **Klein thuis- of kantoornetwerk** – geschikt voor computers in een klein netwerk, bijvoorbeeld thuis of in een klein bedrijf, waar slechts een paar computers met elkaar verbonden zijn, zonder "centrale" beheerder.

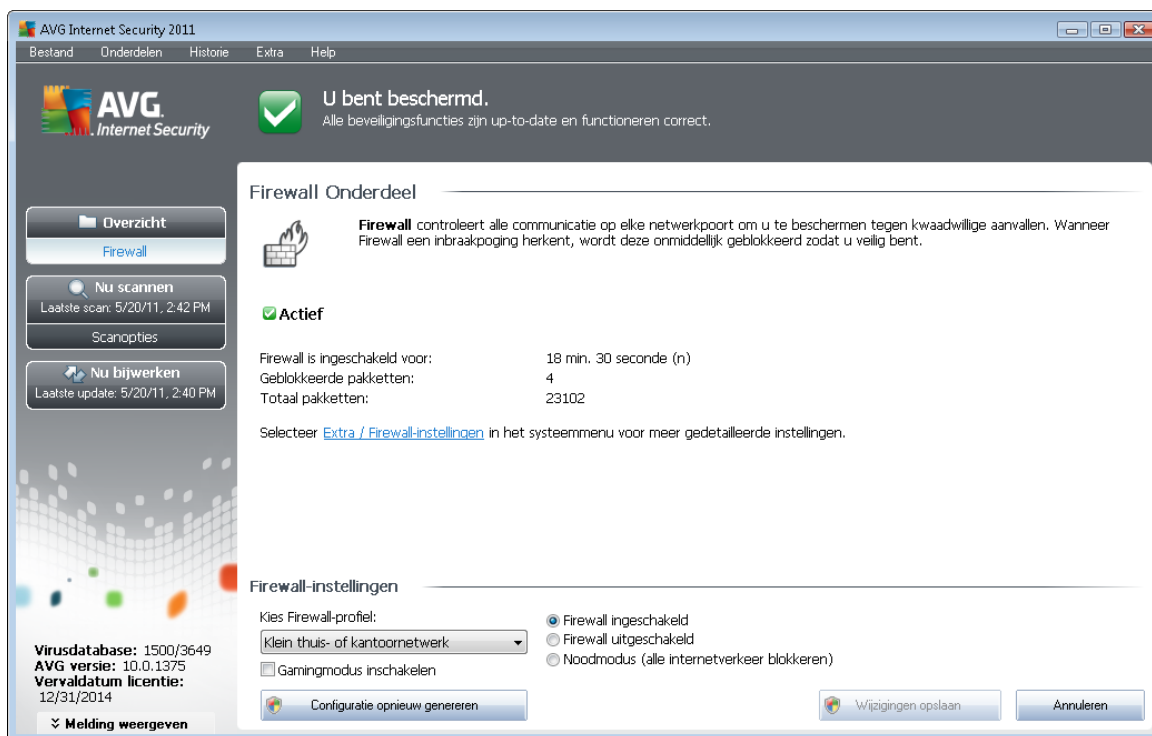
Profiel omschakelen

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

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

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

7.4.3. Firewallinterface



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

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

Firewallinstellingen

- **Kies Firewallprofiel** – selecteer in het vervolgkeuzemenu een van de gedefinieerde profielen – er zijn altijd twee profielen beschikbaar (de *standaardprofielen* **Alles toestaan** en **Blokkeer alles**); daaraan hebt u andere profielen toegevoegd door profielen te wijzigen in het dialoogvenster [Profielen](#) van [Firewallinstellingen](#).
- **Gamingmodus inschakelen** – Schakel deze optie in, zodat u zeker weet dat bij uitvoering van schermvullende toepassingen (*spelletjes, PowerPoint-presentaties, enz.*) de **Firewall** geen dialoogvensters zal openen waarin u wordt gevraagd of u communicatie voor onbekende toepassingen al dan niet wilt toestaan. Als een onbekende toepassing op dat moment probeert te communiceren via het netwerk, zal de **firewall** de poging toestaan of blokkeren, op basis van de instellingen in het huidige profiel. **Opmerking:** Als de



gamingmodus is ingeschakeld, worden alle geplande activiteiten (scans, updates) uitgesteld tot de toepassing wordt afgesloten.

- **Firewallstatus**

- **Firewall ingeschakeld** – selecteer deze optie om communicatie toe te staan aan die toepassingen waarvoor 'toegestaan' is ingesteld in de set regels gedefinieerd voor het geselecteerde [Firewall](#) profiel
- **Firewall uitgeschakeld** – met deze optie schakelt u [Firewall](#) helemaal uit; alle netwerkverkeer is toegestaan en er wordt niet gecontroleerd!
- **Noodmodus (al het internetverkeer blokkeren)** – met deze optie blokkeert u al het verkeer via alle netwerkpoorten; [Firewall](#) is weliswaar actief, maar al het netwerkverkeer is stilgelegd

Opmerking: de leverancier heeft alle onderdelen van AVG zo ingesteld dat ze optimaal presteren. Wijzig de configuratie van AVG niet, tenzij er een goede reden is om dat wel te doen. Wijzigingen in de instellingen dienen alleen te worden uitgevoerd door ervaren gebruikers. Als de noodzaak voor wijziging van de configuratie van Firewall zich voordoet, opent u het menu **Extra / Firewallinstellingen** en wijzigt u de firewallconfiguratie in het dialoogvenster [Firewallinstellingen](#) dat dan wordt geopend.

Knoppen

- **Configuratie regenereren** – de huidige **firewall** configuratie wordt overschreven; het programma keert terug naar de standaardconfiguratie op basis van automatische detectie.
- **Wijzigingen opslaan** – de wijzigingen die u in het dialoogvenster hebt uitgevoerd, worden opgeslagen en toegepast
- **Annuleren** – terugkeren naar de standaard [AVG-gebruikersinterface](#) (het overzicht van onderdelen)

7.5. LinkScanner

7.5.1. LinkScanner principes

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.

De **LinkScanner**-technologie is verdeeld over twee functies, [Search-Shield](#) en [Surf-Shield](#):

- [Search-Shield](#) bevat een lijst met websites (*URL-adressen*) waarvan bekend is dat ze



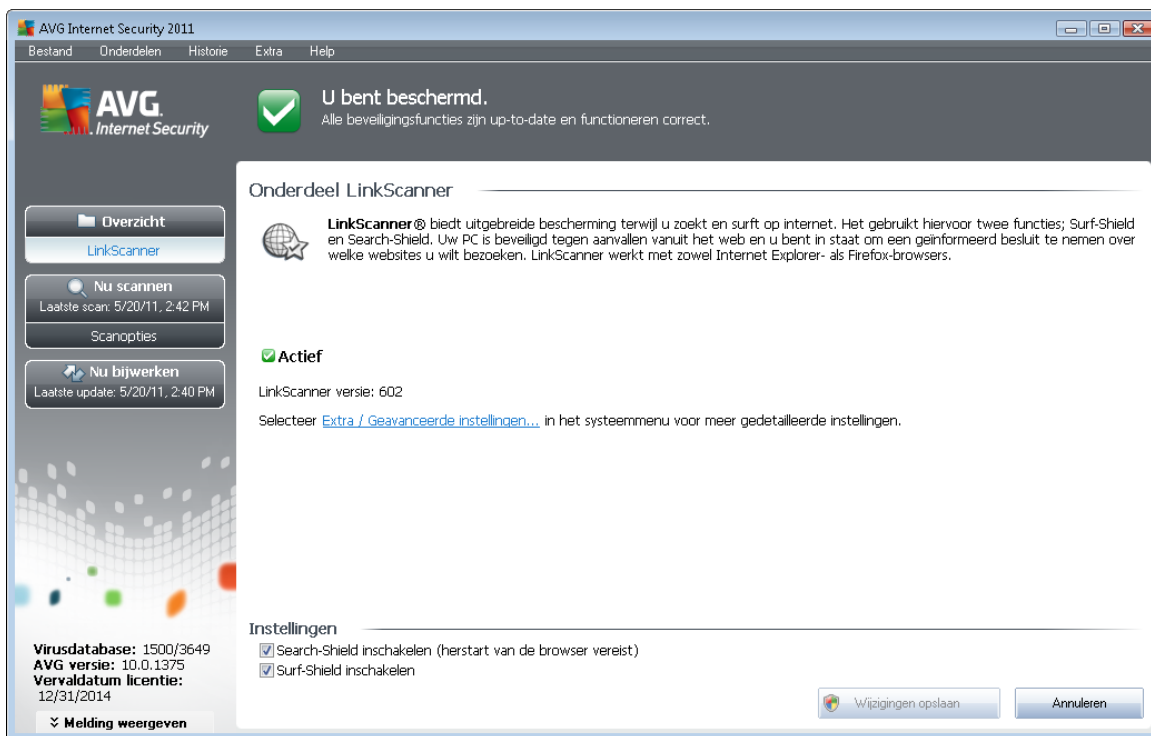
gevaarlijk zijn. Als u zoekt met Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg of SlashDot, worden alle resultaten vergeleken met de lijst en wordt een oordeel weergegeven in de vorm van een pictogram (voor Yahoo wordt alleen een pictogram weergegeven als het oordeel "website met exploit" luidt).

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

Opmerking: LinkScanner is niet bedoeld voor serverplatforms!

7.5.2. Interface LinkScanner

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



LinkScanner-instellingen

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

- **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).

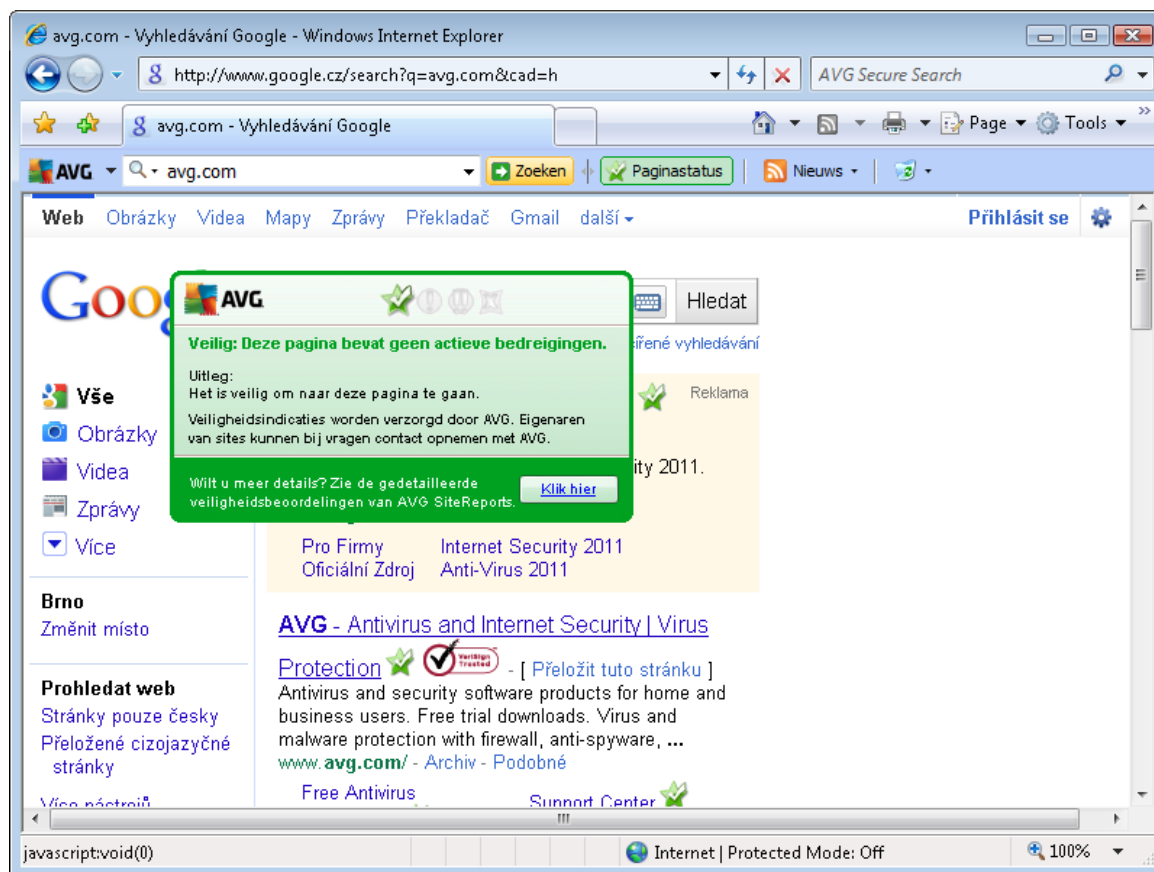
7.5.3. Search-Shield

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. **AVG 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 alleen 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.

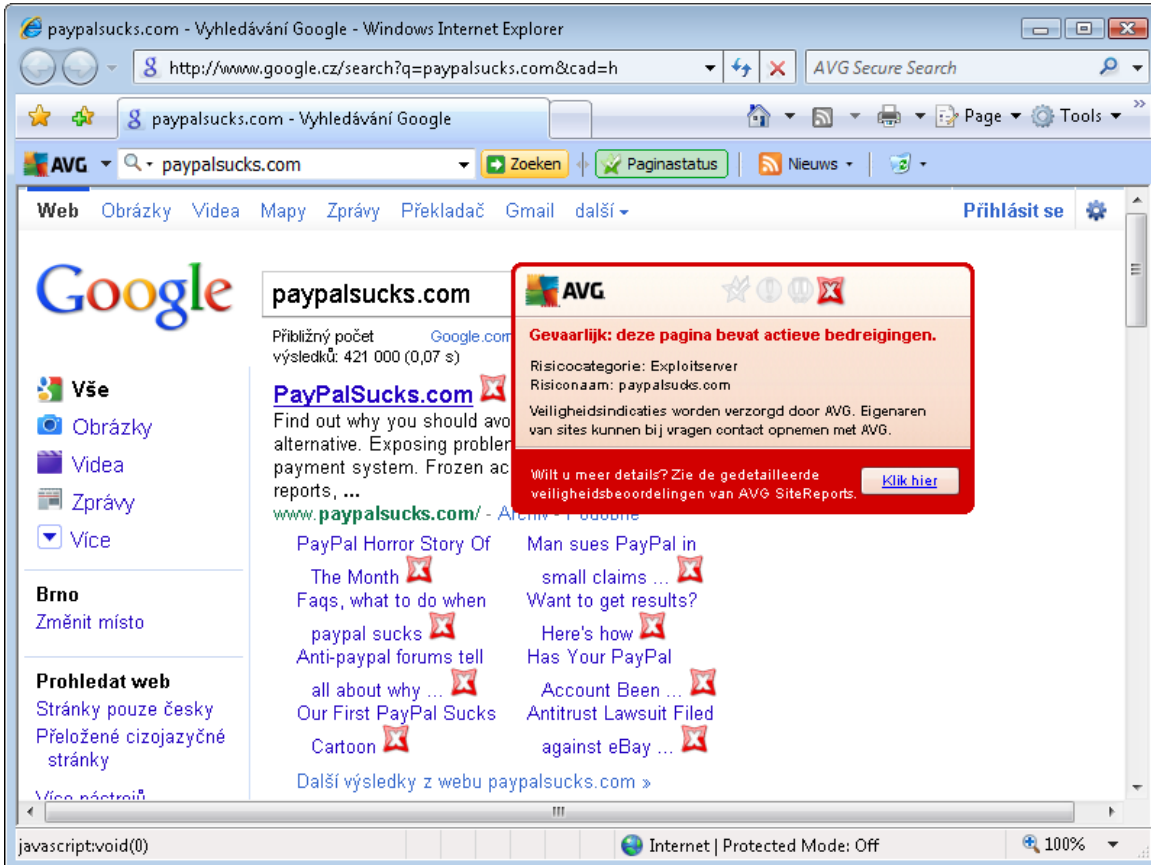
Als u de muisaanwijzer op een pictogram plaatst, worden details van de desbetreffende koppeling weergegeven. Er wordt ook extra informatie gegeven over de bedreiging (als die er is):



7.5.4. Surf-Shield

Dit krachtige schild blokkeert de kwaadaardige inhoud van webpagina's die u probeert te openen en voorkomt dat die naar uw computer wordt gedownload. Als de functie is ingeschakeld, wordt automatisch verhinderd dat een webpagina wordt geopend als u op een koppeling klikt of de URL typt van een gevaarlijke site, en zo wordt voorkomen dat u per ongeluk geïnfecteerd raakt. Het is belangrijk te weten dat webpagina's met een exploit uw computer kunnen infecteren, alleen al als u de desbetreffende site bezoekt; om die reden zal de [AVG LinkScanner](#) verhinderen dat uw webbrowswer gevaarlijke webpagina's met exploits of andere serieuze bedreigingen weergeeft.

Als u wordt geconfronteerd met een kwaadaardige website, wordt u door de [AVG Link Scanner](#) gewaarschuwd met een scherm als het volgende:



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

7.6. Resident Shield

7.6.1. Resident Shield principes

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

Resident Shield kan het volgende doen:

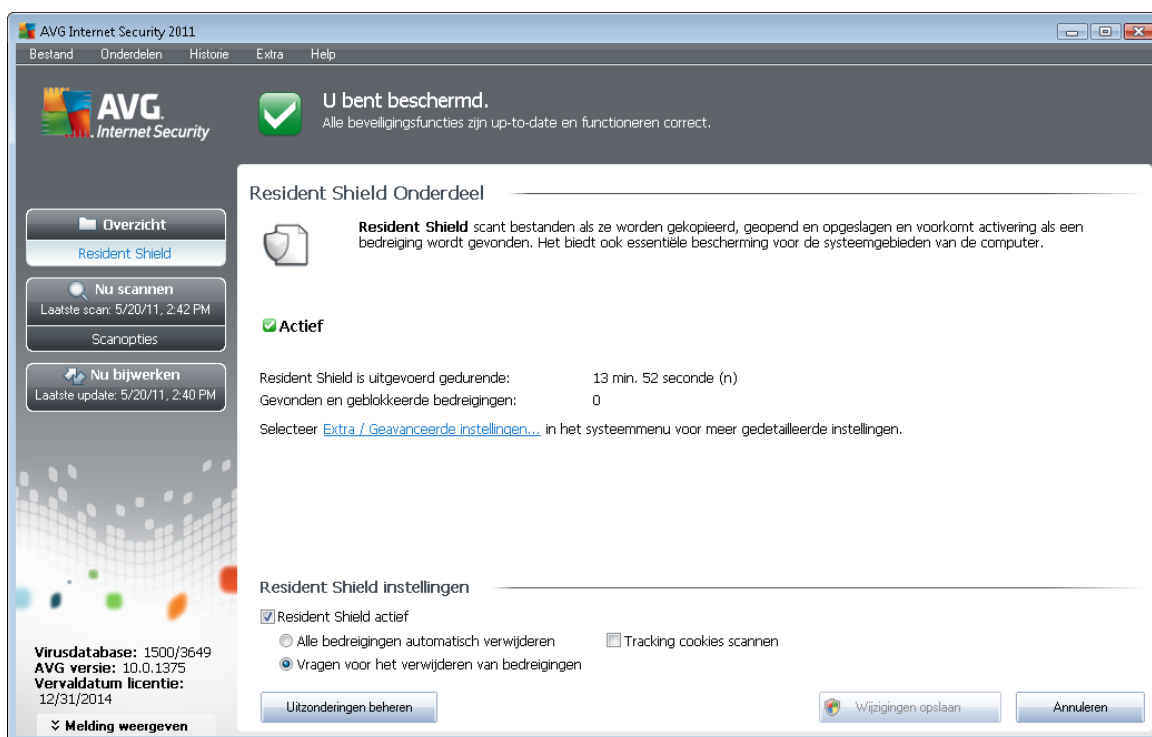
- Scannen naar specifieke soorten potentiële bedreigingen
- Verwisselbare media scannen (*flash-discs, enz.*)



- Bestanden scannen met specifieke extensies of zelfs zonder extensies
- Bestanden uitzonderen van scannen – u kunt bestanden opgeven die Resident Shield nooit hoeft te scannen

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

7.6.2. Resident Shield interface



Naast een overzicht van de functionaliteit van **Resident Shield** en informatie over de status van het onderdeel, staat er ook enig cijfermateriaal in de interface van **Resident Shield** :

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

Resident Shield Instellingen

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



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

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

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

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

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

Knoppen

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

- **Uitzonderingen beheren** – als u op deze knop klikt, wordt het dialoogvenster [Resident Shield uitsluitingen](#) geopend, waarin u mappen kunt opgeven die niet door [Resident Shield](#) moeten worden gescand
- **Wijzigingen opslaan** – klik op deze knop om de wijzigingen die u in het dialoogvenster hebt uitgevoerd op te slaan en toe te passen
- **Annuleren** – terugkeren naar de standaard [AVG-gebruikersinterface](#) (het overzicht van onderdelen)

7.6.3. Resident Shield detectie

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



In 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 [Virus encyclopedie](#) met gedetailleerde informatie over het gedetecteerde virus, indien bekend (*Meer informatie*).

Bovendien zult u moeten besluiten welke actie nu moet worden ondernomen – u kunt kiezen uit de volgende opties:

Welke knoppen beschikbaar zijn, is afhankelijk van de omstandigheden (het soort bestand dat is geïnfecteerd, de locatie van het bestand, enz.).

- **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 [Quarantaine](#)*)
- **Naar quarantaine verplaatsen** – het virus zal worden verplaatst naar de AVG [Quarantaine](#)
- **Ga naar bestand** – u wordt verwezen naar de exacte locatie van het verdachte object (*er wordt een nieuw Verkennervenster geopend*)
- **Negeren** – we raden u met nadruk aan deze optie NIET te kiezen tenzij u een heel goede reden hebt om dat wel te doen!

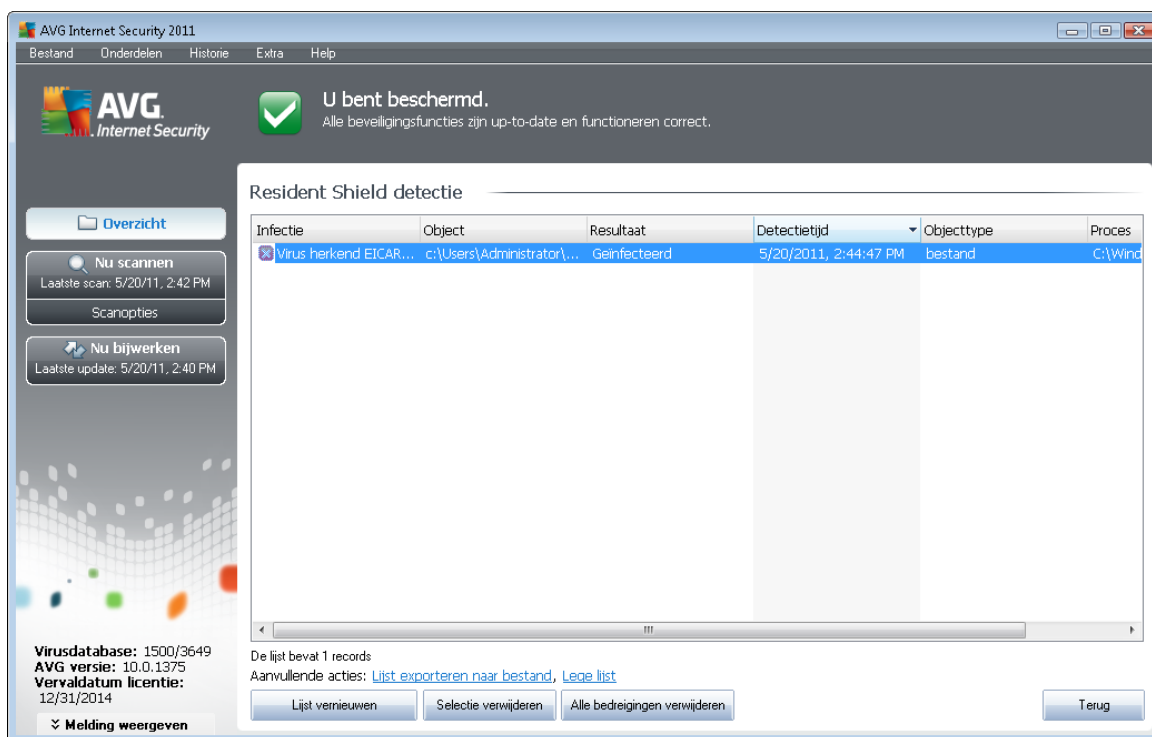
Opmerking: mogelijk is het gedetecteerde object te groot voor de beschikbare capaciteit van de Quarantaine. Als dat gebeurt wordt in een berichtvenster melding van het feit gemaakt op het



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.

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 de standaard [AVG-gebruikersinterface](#) (*Overzicht van onderdelen*).

7.7. Veiligheid voor het gezin

AVG 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 van bescherming instellen en hen afzonderlijk volgen met behulp van unieke aanmeldingen.

Het onderdeel is alleen actief als **AVG Family Safety** op uw apparaat is geïnstalleerd. Als **AVG Family Safety** niet is geïnstalleerd, klikt u op het desbetreffende pictogram in de gebruikersinterface van **AVG Internet Security 2011** ; u wordt dan omgeleid naar de website van het product waar u alle vereiste informatie vindt.

7.8. AVG LiveKive

AVG LiveKive automatische back-ups van al uw bestanden, foto's en muziek op één veilige plaats, zodat u ze kunt delen met familie en vrienden, bereikbaar vanaf elk apparaat met toegang tot internet, ook iPhones en apparaten met Android.

Het onderdeel is alleen actief als **AVG LiveKive** op uw apparaat is geïnstalleerd. Als **AVG LiveKive** niet is geïnstalleerd, klikt u op het desbetreffende pictogram in de gebruikersinterface van **AVG Internet Security 2011** ; u wordt dan omgeleid naar de website van het product waar u alle vereiste informatie vindt.

7.9. E-mailscanner

E-mail is een van de belangrijkste bronnen voor virussen en Trojaanse paarden. Phishing en spam maken van e-mail een nog grotere risicofactor. Gratis e-mailaccounts hebben meer last van dergelijke kwaadaardige e-mail (*omdat daar zelden anti-spamtechnologie wordt toegepast*), terwijl thuisgebruikers daar veelal van afhankelijk zijn. Thuisgebruikers stellen zich ook vaak gemakkelijk bloot aan aanvallen via e-mail, omdat ze op onbekende sites surfen en op online formulieren persoonlijke gegevens (*bijvoorbeeld het e-mailadres*) invullen. Bedrijven maken meestal gebruik van bedrijfsaccounts voor e-mail en schakelen spamfilters e.d. in om de risico's in te dammen.

7.9.1. E-mailscanner principes

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.



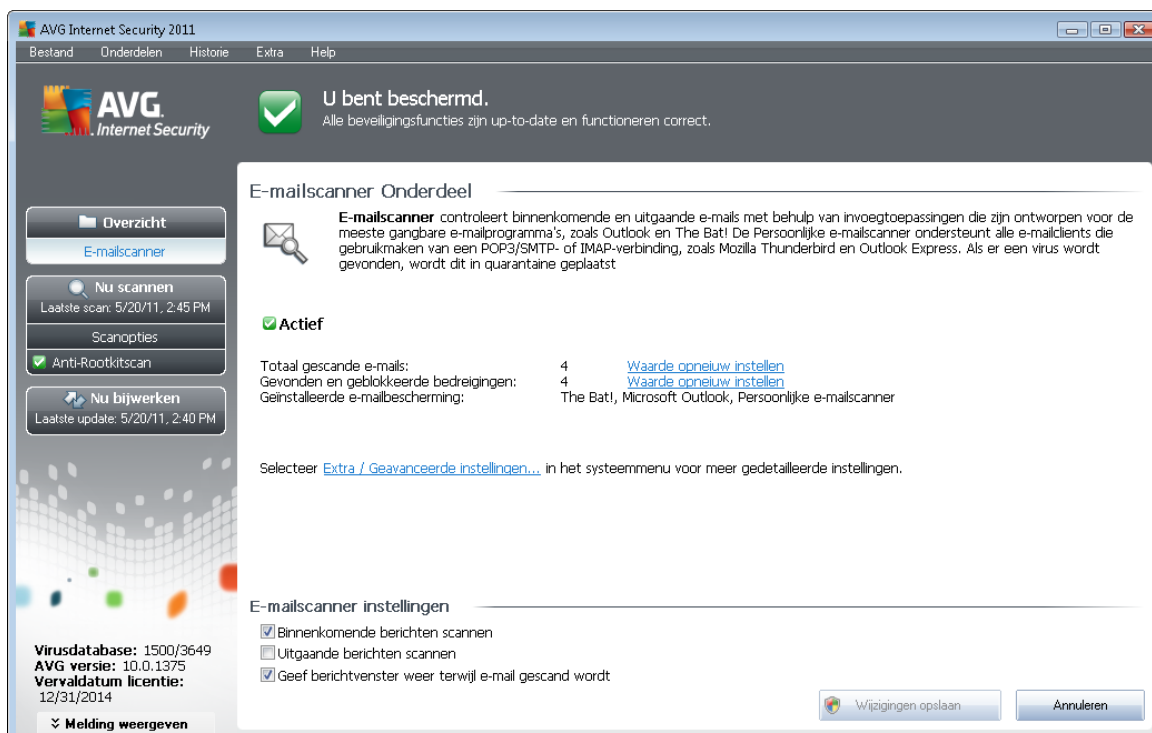
Bij de [installatie](#) van AVG worden automatische servers gecreëerd voor controle van e-mail: één voor het controleren van binnenkomende e-mail en één voor het controleren van uitgaande e-mails. Met behulp van deze twee servers worden e-mails automatisch gecontroleerd op de poorten 110 en 25 (standaardpoorten 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 [Quarantaine](#). Vervolgens wordt het bericht doorgestuurd naar de e-mailclient.
- **Uitgaande e-mail:** het bericht wordt door de e-mailclient verstuurd naar de E-mailscanner; daar wordt het bericht met de bijlagen gescand op virussen, waarna het naar de SMTP-server wordt gestuurd (*scannen van uitgaande e-mail is standaard uitgeschakeld, maar kan handmatig worden ingesteld*).

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

7.9.2. E-mailscanner interface



Op het scherm van het onderdeel **E-mailscanner** staat een korte tekst met een beschrijving van de functie van het onderdeel, informatie over de huidige status en het volgende cijfermateriaal:

- **Totaal gescande e-mails:** – het aantal gescande e-mailberichten sinds de laatste keer dat **E-mailscanner** is gestart (*desgewenst kan deze waarde opnieuw worden ingesteld, bijvoorbeeld voor statistische doeleinden – Waarde opnieuw instellen*)



- **Gevonden en geblokkeerde bedreigingen** – het aantal in e-mailberichten gedetecteerde infecties sinds de laatste keer dat **E-mailscanner** is gestart
- **Geïnstalleerde e-mailbescherming** – informatie over een specifieke invoegtoepassing voor e-mailbescherming die verwijst naar uw standaard e-mailclient

E-mailscanner instellingen

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

- **Binnenkomende berichten scannen** – schakel het selectievakje bij deze optie in om op te geven dat alle e-mailberichten die aan uw account zijn gericht, moeten worden gescand op virussen. Standaard is deze optie ingeschakeld en het wordt aanbevolen deze niet uit te schakelen.
- **Uitgaande berichten scannen** – schakel het selectievakje bij deze optie in om op te geven dat alle e-mailberichten die via uw account worden verzonden, moeten worden gescand op virussen. De optie is standaard uitgeschakeld.
- **Waarschuwingspictogram weergeven bij het scannen van e-mail** – schakel deze optie in als u informatie wilt krijgen via een waarschuwingspictogram dat over het AVG-pictogram in het systeemvak wordt weergegeven tijdens het scannen van uw mail met het onderdeel **E-mailscanner**. Standaard is de optie ingeschakeld en het wordt aanbevolen deze niet uit te schakelen.

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

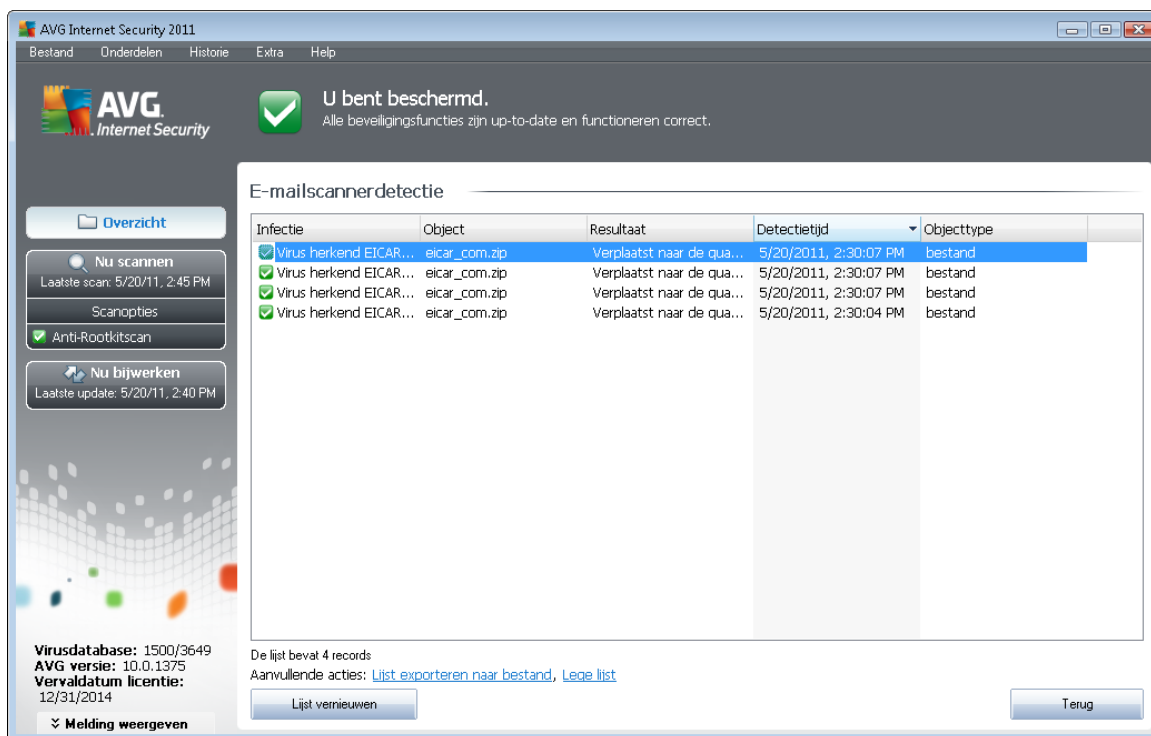
Opmerking: de leverancier heeft alle onderdelen van AVG zo ingesteld dat ze optimaal presteren. Wijzig de configuratie van AVG niet, tenzij er een goede reden is om dat wel te doen. Wijzigingen in de instellingen dienen alleen te worden uitgevoerd door ervaren gebruikers. Als u de AVG-configuratie dient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

Knoppen

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

- **Wijzigingen opslaan** – klik op deze knop om de wijzigingen die u in het dialoogvenster hebt aangebracht op te slaan en toe te passen
- **Annuleren** – terugkeren naar de standaard [AVG-gebruikersinterface](#) (het overzicht van onderdelen)

7.9.3. E-mailscanner detectie



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

- **Infectie** – beschrijving (indien mogelijk de naam) van het gedetecteerde object
- **Object** – locatie van het object
- **Resultaat** – de bewerking die met het gedetecteerde object is uitgevoerd
- **Detectietijd** – datum en tijdstip waarop het object is gedetecteerd
- **Objecttype** – type van het gedetecteerde object

In het onderste gedeelte van het dialoogvenster, onder de lijst, vindt u informatie over het totale aantal gedetecteerde objecten dat 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** – de lijst met gedetecteerde bedreigingen bijwerken met nieuwe gegevens



- **Terug** – terugkeren naar het vorige weergegeven dialoogvenster

7.10. Updatebeheer

7.10.1. Updatebeheer principes

Geen enkel beveiligingsprogramma kan werkelijk garant staan voor bescherming tegen allerlei bedreigingen als het niet regelmatig wordt bijgewerkt! De makers van virussen zoeken steeds naar nieuwe tekortkomingen in software en besturingssystemen om uit te buiten. Elke dag verschijnen er nieuwe virussen, nieuwe malware en nieuwe hacker-aanvallen. Om die reden laten de leveranciers van software steeds nieuwe updates en beveiligingspatches verschijnen, om de gaten te dichten die in de beveiliging zijn ontdekt.

Het is cruciaal dat u regelmatig updates uitvoert voor AVG.

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

Opmerking: neem het hoofdstuk [AVG Updates](#) door voor meer informatie over typen updates en updateniveaus!

7.10.2. Updatebeheer interface



In de interface van **Updatebeheer** staat informatie over de functionaliteit van het onderdeel, de huidige status en enig cijfermateriaal:

- **Laatste update** – datum en tijdstip van de laatste update van de database
- **Virusdatabaseversie** – het nummer van de laatste virusdatabaseversie; dit nummer wordt bij iedere nieuwe versie één hoger
- **Volgende geplande update** – datum en tijdstip van de eerstvolgende update van de database

Updatebeheer instellingen

Het onderste deel van het dialoogvenster is de sectie **Instellingen Updatebeheer** waar u een aantal wijzigingen kunt aanbrengen in de regels die het starten van de updateprocedure bepalen. U kunt opgeven dat updatebestanden automatisch moeten worden gedownload (**Automatische updates starten**) of alleen op verzoek. Standaard is de optie **Automatische updates starten** ingeschakeld; het is raadzaam die instelling aan te houden! Het regelmatig downloaden van de nieuwste updates is cruciaal voor het goed functioneren van welke vorm van beveiligingssoftware dan ook!

Bovendien bepaalt u hier wanneer de opstartprocedure moet worden gestart:

- **Periodiek** – geef een tijdsinterval op
- **Op een specifiek tijdstip** – geef een moment van de dag op voor het starten van de update

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

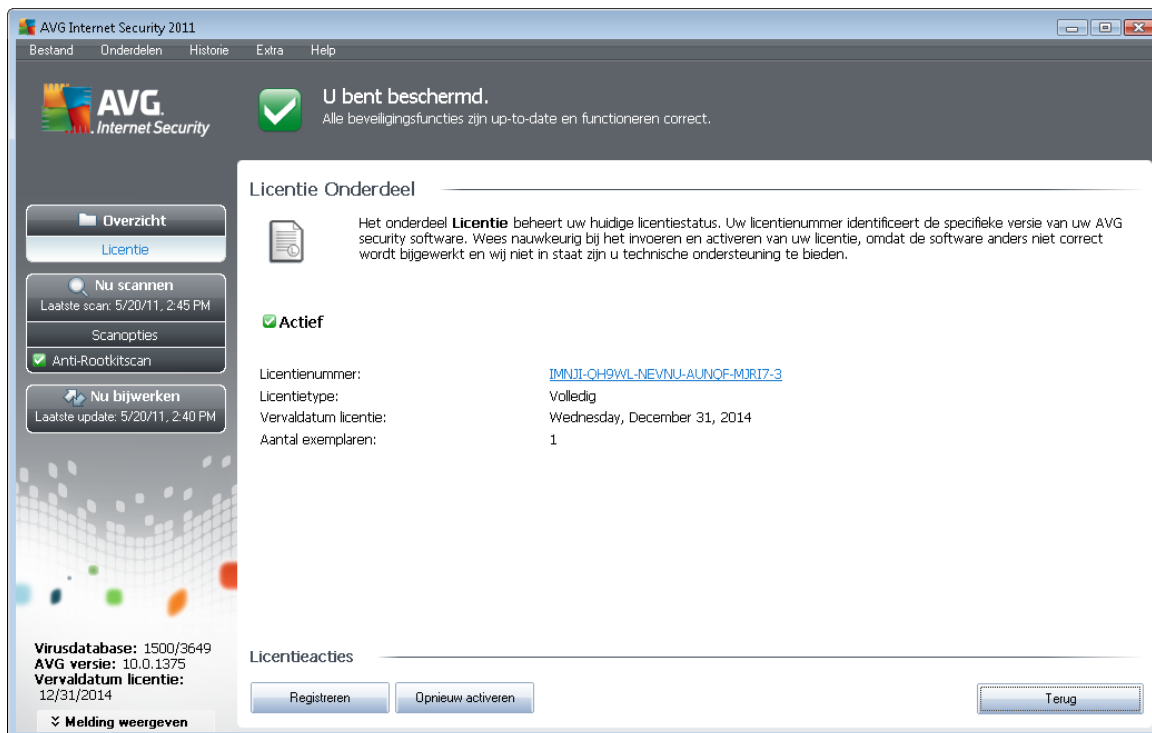
Opmerking: de leverancier heeft alle onderdelen van AVG zo ingesteld dat ze optimaal presteren. Wijzig de configuratie van AVG niet, tenzij er een goede reden is om dat wel te doen. Wijzigingen in de instellingen dienen alleen te worden uitgevoerd door ervaren gebruikers. Als u de AVG-configuratie dient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

Knoppen

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

- **Nu bijwerken** – op verzoek wordt een [onmiddellijke update](#) uitgevoerd
- **Wijzigingen opslaan** – de wijzigingen die u in het dialoogvenster hebt aangebracht opslaan en toepassen
- **Annuleren** – terugkeren naar de standaard [AVG-gebruikersinterface](#) (het overzicht van onderdelen)

7.11. Licentie



Op het scherm van het onderdeel **Licentie** staat een korte tekst met een beschrijving van de functionaliteit van het onderdeel, informatie over de huidige status en de volgende informatie:

- **Licentienummer** – de verkorte vorm van het licentienummer (*om veiligheidsredenen ontbreken de laatste vier cijfers*). Als u uw licentienummer invoert, dient u het heel nauwkeurig zo te typen als het wordt weergegeven. We raden u dan ook met nadruk aan bij alle bewerkingen met het licentienummer de methode "knippen-en-plakken" toe te passen.
- **Licentietype** – het type geïnstalleerd product.
- **Vervaldatum licentie** – de datum waarop de licentie zijn geldigheid verliest. Als u **AVG Internet Security 2011** wilt blijven gebruiken na die datum, moet u uw licentie verlengen. U kunt de licentie online verlengen op de [website van AVG](#).
- **Aantal exemplaren** – het aantal werkstations waarop u **AVG Internet Security 2011** mag installeren.

Knoppen

- **Registreren** – verbinding maken met de registratiepagina van de website van AVG (<http://www.avg.com/>). Voer uw registratiegegevens in; alleen klanten die hun AVG-product registreren komen in aanmerking voor gratis technische ondersteuning.
- **Opnieuw activeren** – het dialoogvenster **AVG activeren** wordt geopend met de gegevens die u hebt opgegeven in het dialoogvenster **AVG aanpassen** van de [installatieprocedure](#). In

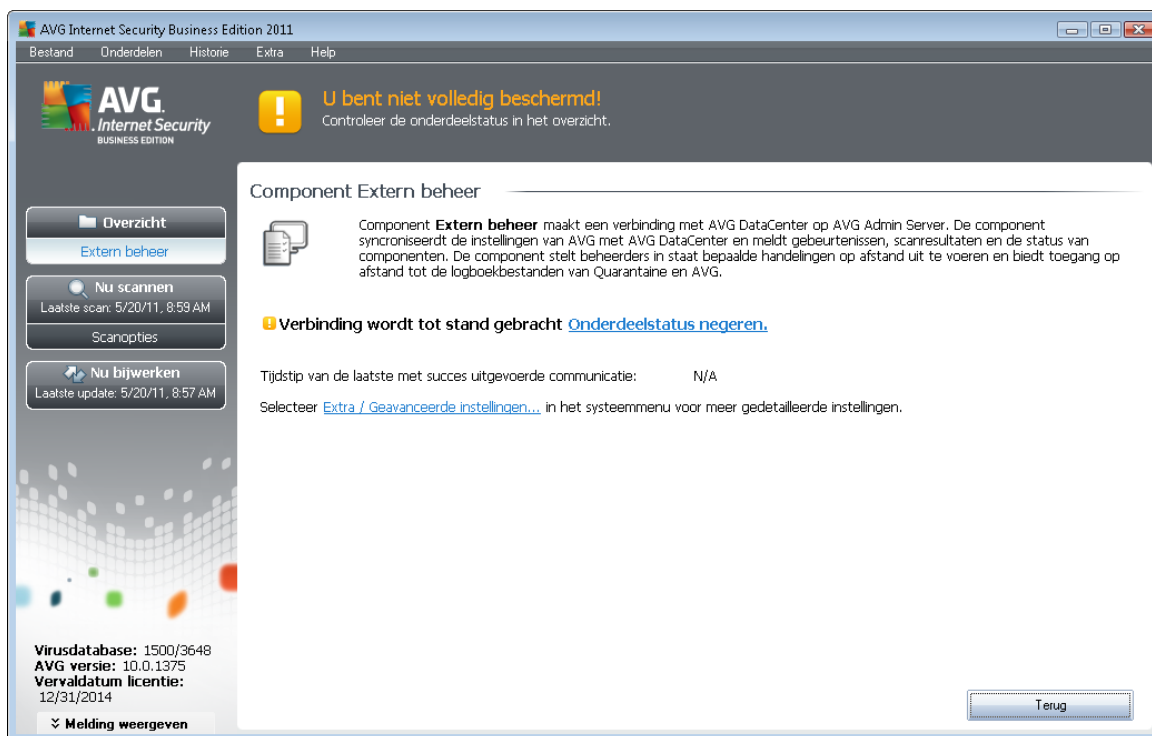


dit dialoogvenster kunt u uw licentienummer invoeren ter vervanging van ofwel het verkoopnummer (*het nummer waarmee u AVG hebt geïnstalleerd*), ofwel het oude licentienummer (*bijvoorbeeld bij het upgraden naar een nieuw product van AVG*).

Opmerking: als u de proefversie van *AVG Internet Security 2011* gebruikt, worden de knoppen weergegeven als **Nu kopen en Activeren**, zodat u de volledige versie van het programma meteen kunt kopen. Als u *AVG Internet Security 2011* hebt geïnstalleerd met een verkoopnummer, worden deze knoppen weergegeven als **Registreren en Activeren**.

- **Terug** – Terugkeren naar de standaard [AVG-gebruikersinterface](#) (het overzicht van onderdelen).

7.12. Extern beheer



Het onderdeel **Extern beheer** wordt alleen weergegeven in de gebruikersinterface van **AVG Internet Security 2011** als u de Business Edition van het product hebt geïnstalleerd (zie het onderdeel [Licentie](#)). In het dialoogvenster **Extern beheer** staat informatie over het al dan niet actief zijn van het onderdeel en de verbinding met een server. All 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 die documentatie downloaden van de [website van AVG \(www.avg.com\)](http://www.avg.com) in het gedeelte **Support center / Downloaden / Documentatie**.

Knoppen



- **Terug** – terugkeren naar de standaard [AVG gebruikersinterface](#) (het overzicht van onderdelen).

7.13. Online Shield

7.13.1. Online Shield principes

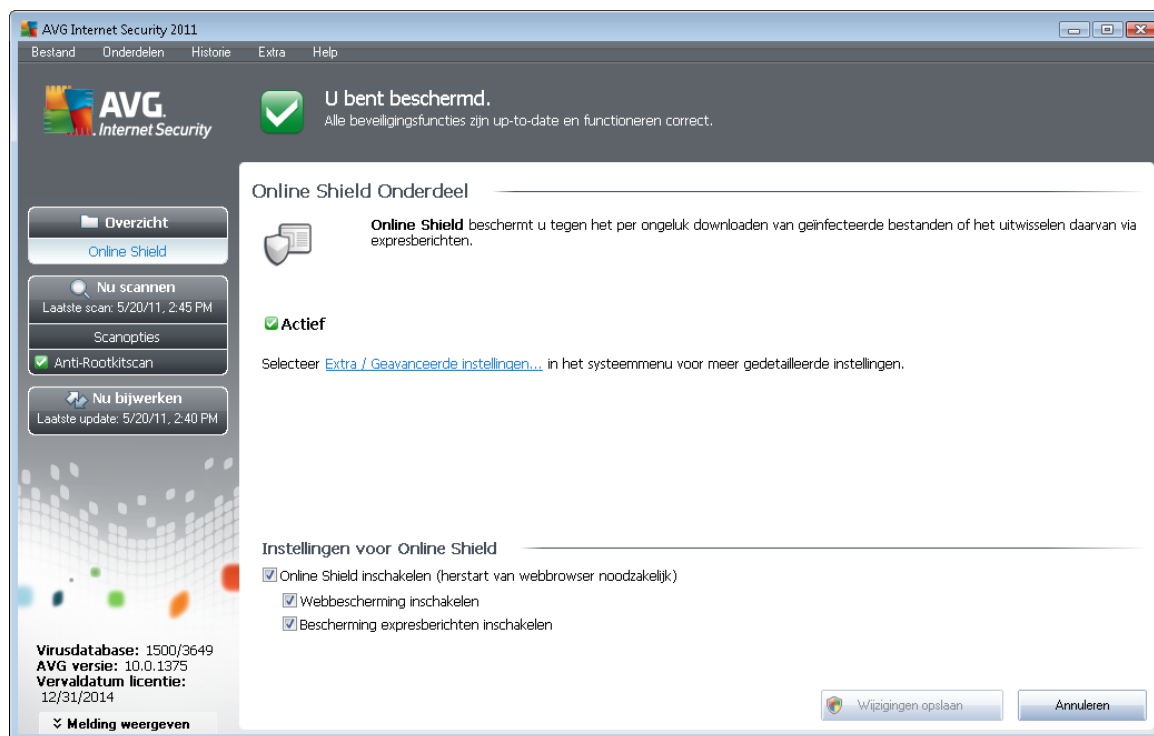
Online Shield is een vorm van interne, real-time bescherming; de inhoud van bezochte webpagina's (en van de bestanden die daarvan eventueel deel uitmaken) wordt gescand zelfs voordat deze wordt weergegeven in uw webbrowser of wordt gedownload naar uw computer.

Als Online Shield detecteert dat de pagina die u wilt gaan bezoeken, bijvoorbeeld een gevaarlijk Javascript bevat, wordt weergave van die pagina verhinderd. Bovendien herkent het malware op pagina's en verhindert het onmiddellijk dat de malware wordt gedownload, zodat de malware uw computer nooit bereikt.

Opmerking: AVG Online Shield is niet bedoeld voor serverplatforms!

7.13.2. Online Shield interface

De interface van het onderdeel **Online Shield** beschrijft wat dit type bescherming doet. Er staat bovendien informatie over de huidige status van het onderdeel. In het onderste deel van het dialoogvenster staan de elementaire bewerkingsopties voor het functioneren van het onderdeel.



Instellingen Online Shield

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

- **Webbescherming inschakelen** – met deze optie geeft u op of **Online Shield** de inhoud van webpagina's moet scannen.
- **Bescherming voor expresberichten inschakelen** – **Online Shield** controleert of de communicatie met expresberichten (*dat wil zeggen via ICQ, MSN Messenger, ...*) virusvrij verloopt.

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

Knoppen

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

- **Wijzigingen opslaan** – de wijzigingen die u in het dialoogvenster hebt aangebracht opslaan en toepassen
- **Annuleren** – terugkeren naar de standaard [AVG-gebruikersinterface](#) (het overzicht van onderdelen)

7.13.3. Online Shield detectie

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



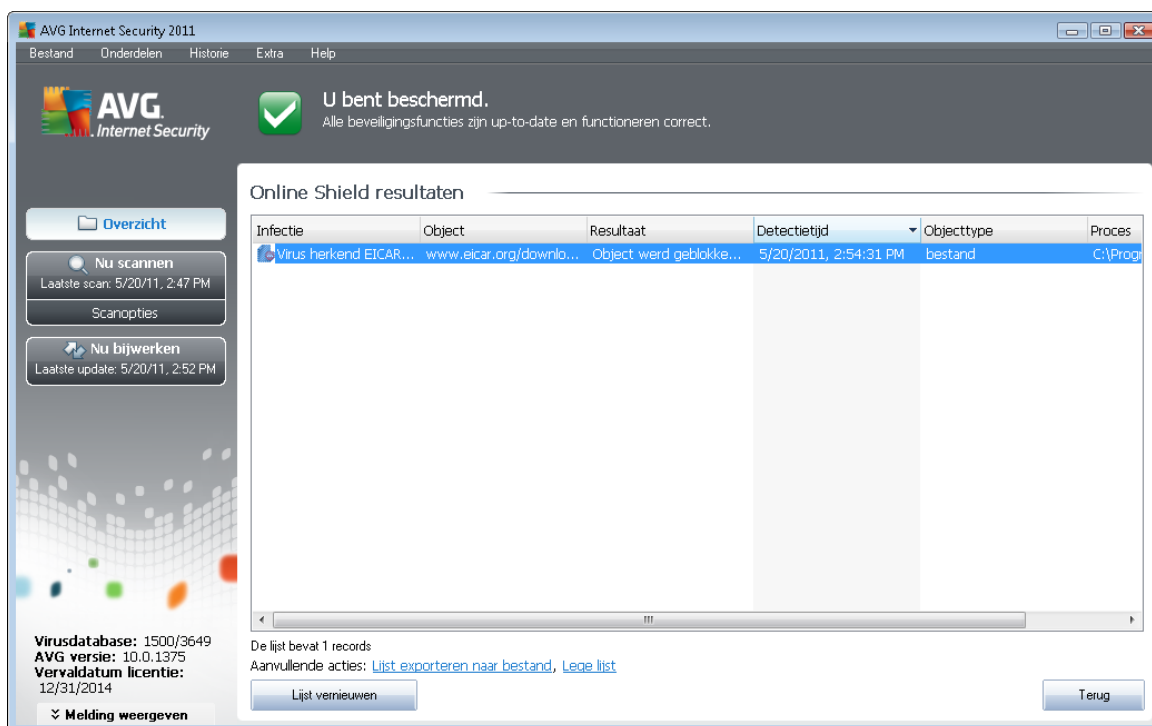
In dit waarschuwingsvenster staan gegevens over het bestand dat is gedetecteerd als geïnfecteerd (



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**). Als u op de knop **Lijst vernieuwen** klikt, wordt de lijst met door **Online Shield** gedetecteerde items vernieuwd. Als u op de knop **Terug** klikt, keert u terug naar de standaard [AVG-gebruikersinterface](#) (*Overzicht van onderdelen*).

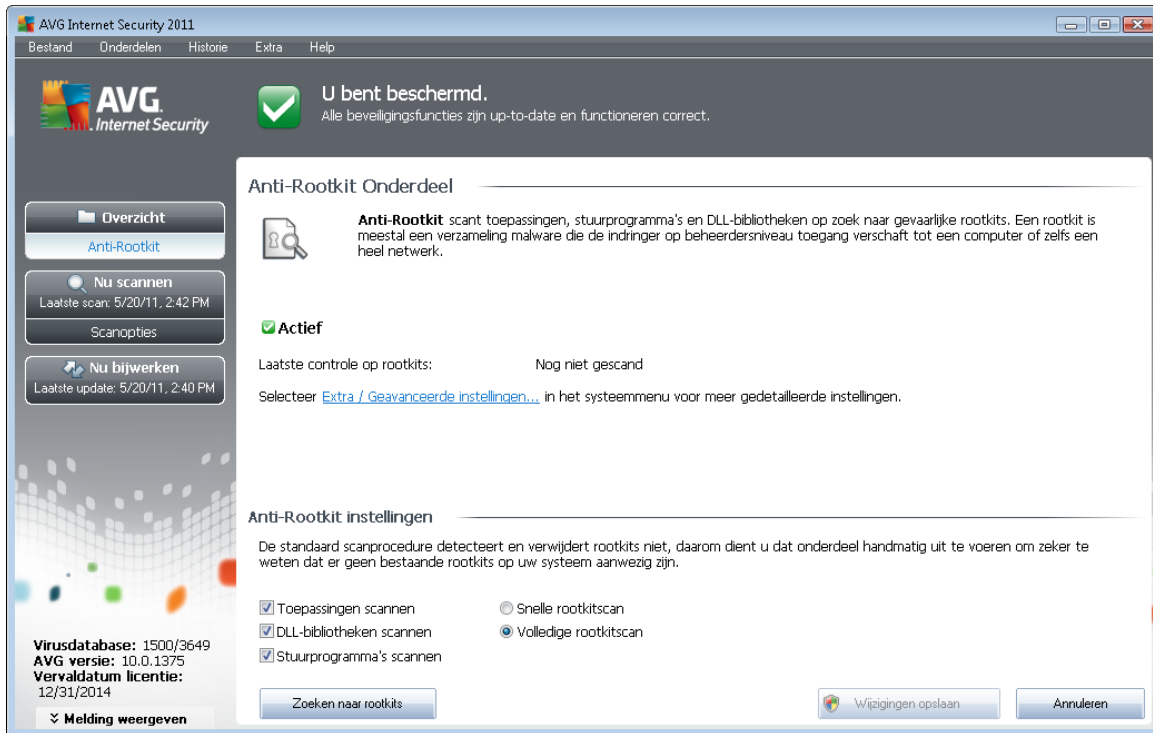
7.14. Antirookit

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.

7.14.1. Antirookit principes

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

7.14.2. Antirookit interface



De gebruikersinterface van **Anti-Rootkit** geeft een beknopte beschrijving van de functionaliteit van het onderdeel, geeft informatie over de huidige status van het onderdeel en informatie over de laatste keer dat de **Anti-Rootkit** scan 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.

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

Anti-rootkit Instellingen

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

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

Vervolgens kunt u de scanmodus kiezen:



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

Knoppen

- **Zoeken naar rootkits** – aangezien de rootkitscan geen geïntegreerd onderdeel is van [Volledige computer scannen](#), kunt u rechtstreeks vanuit de **Anti-rootkit**-interface rootkitscans uitvoeren als u op deze knop klikt.
- **Wijzigingen opslaan** – klik op deze knop om alle wijzigingen die u in dit venster hebt uitgevoerd op te slaan en terug te keren naar de standaard [AVG-gebruikersinterface](#) (*Overzicht van onderdelen*)
- **Annuleren** – druk op deze knop om terug te keren naar de standaard [AVG-gebruikersinterface](#) (*Overzicht van onderdelen*) zonder wijzigingen op te slaan

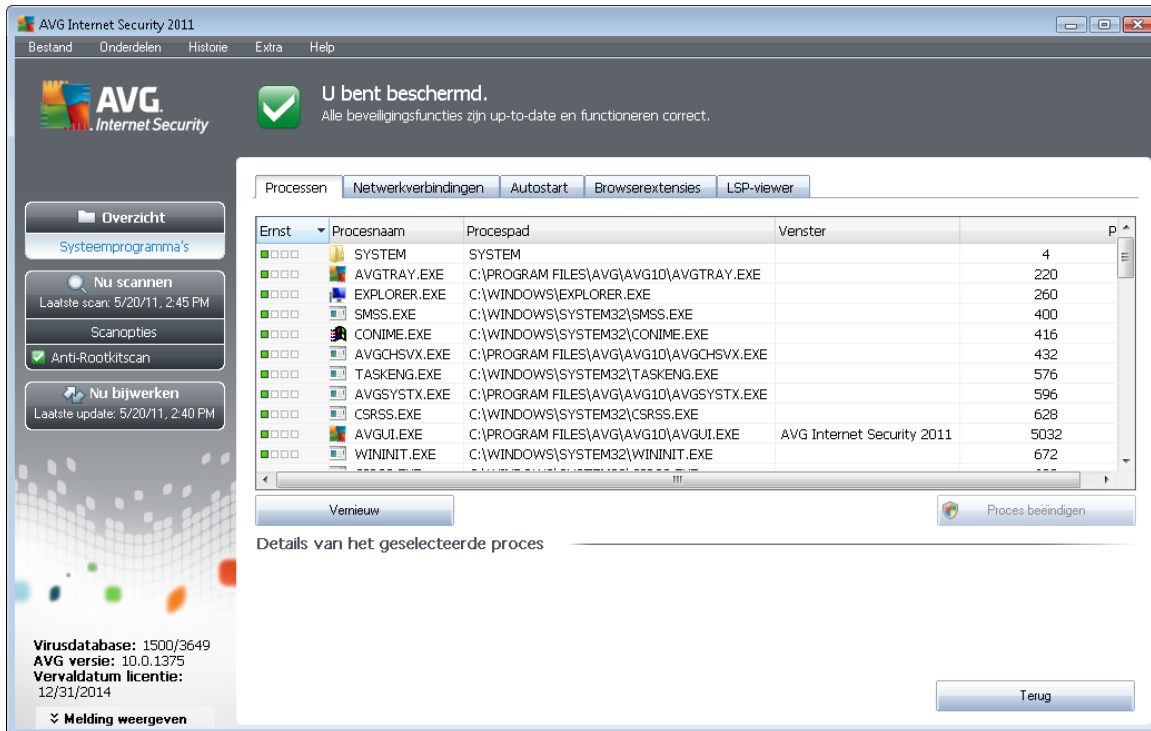
7.15. Systeemprogramma's

Systeemprogramma's verwijst naar een gedetailleerd overzicht van de omgeving van **AVG Internet Security 2011** en het besturingssysteem. In dit onderdeel vindt u een overzicht van:

- [Processen](#) – een lijst met processen (*bijv. toepassingen die worden uitgevoerd*) die op het moment van raadplegen actief zijn op de computer
- [Netwerkverbindingen](#) – lijst met op het moment van raadplegen actieve verbindingen
- [Autostart](#) – een lijst met alle toepassingen die worden uitgevoerd tijdens het opstarten van het Windows-systeem
- [Browserextensies](#) – een lijst met invoegtoepassingen (*bijvoorbeeld toepassingen*) die zijn geïnstalleerd in uw internetbrowser.
- [LSP-viewer](#) – een lijst met Layered Service Providers (*LSP's*)

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

7.15.1. Processen



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

- **Bedreigingsniveau** – grafische aanduiding voor het bedreigingsniveau van het proces op een schaal met vier niveaus van vrij onbelangrijk (■□□□) tot kritiek (■□□■)
- **Procesnaam** – de naam van het proces dat momenteel wordt uitgevoerd
- **Pad** – het fysieke pad naar het proces dat wordt uitgevoerd
- **Venster** – indien van toepassing, de naam van het toepassingsvenster
- **PID** – het PID (process identification number) is een uniek intern nummer waarmee Windows het proces aanduidt

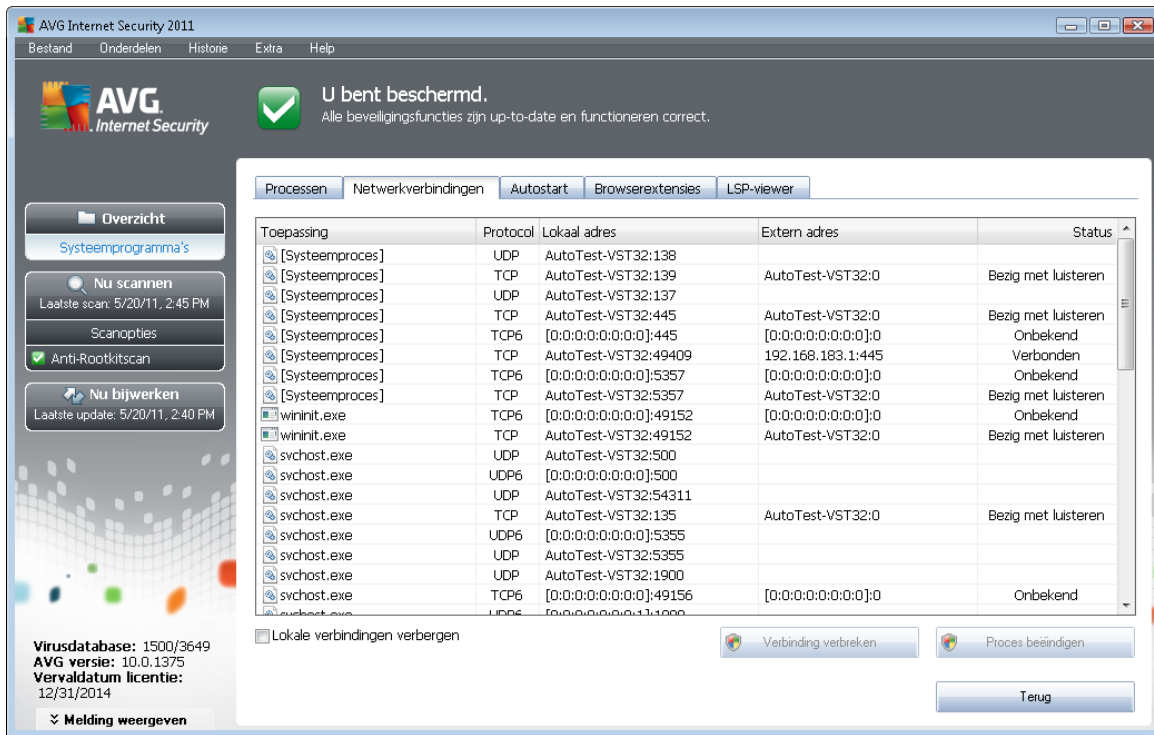
Knoppen

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

- **Vernieuwen** – de lijst met processen bijwerken aan de hand van de huidige status
- **Proces beëindigen** – u kunt één of meer toepassingen selecteren en die beëindigen door op deze knop te klikken. **Het beëindigen van toepassingen raden we u ten zeerste af, tenzij u absoluut zeker weet dat deze toepassingen een bedreiging vormen!**

- **Terug** – terugkeren naar de standaard [AVG-gebruikersinterface](#) (Overzicht van onderdelen)

7.15.2. Netwerkverbindingen



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

- **Toepassing** – naam van de toepassing met betrekking tot de verbinding (*met uitzondering van Windows 2000 waarin deze informatie niet beschikbaar is*)
- **Protocol** – transmissieprotocoltype dat voor de verbinding wordt gebruikt:
 - TCP – het protocol dat samen met het Internet Protocol (IP) wordt gebruikt om informatie over het internet te verzenden
 - UDP – een alternatief voor het TCP-protocol
- **Lokaal adres** – IP-adres en het gebruikte poortnummer van de lokale computer
- **Extern adres** – IP-adres en poortnummer van de externe computer waarmee een verbinding bestaat. Zo mogelijk wordt ook de hostnaam van de externe computer opgezocht.
- **Status** – de meest waarschijnlijke huidige status (*Verbonden, Server moet worden afgesloten, Luisteren, Actieve afsluiting voltooid, Passieve afsluiting, Actieve afsluiting*)

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

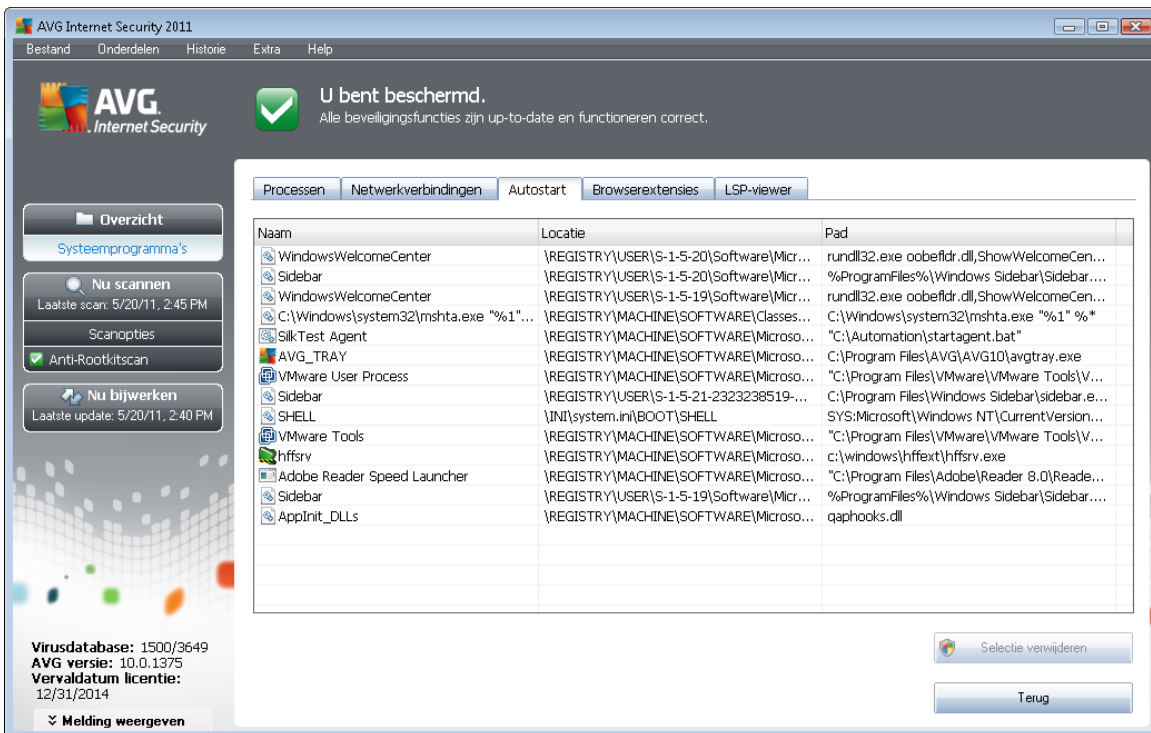
Knoppen

De beschikbare knoppen zijn:

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

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

7.15.3. Autostart



The screenshot shows the AVG Internet Security 2011 interface. The main window title is "AVG Internet Security 2011" and the status bar indicates "U bent beschermd." (You are protected). The "Autostart" tab is selected, displaying a list of applications that start automatically with Windows. The list has three columns: "Naam" (Name), "Locatie" (Location), and "Pad" (Path).

Naam	Locatie	Pad
WindowsWelcomeCenter	\REGISTRY\USER\S-1-5-20\Software\Micr...	rundll32.exe oobefldr.dll,ShowWelcomeCen...
Sidebar	\REGISTRY\USER\S-1-5-20\Software\Micr...	%ProgramFiles%\Windows Sidebar\Sidebar...
WindowsWelcomeCenter	\REGISTRY\USER\S-1-5-19\Software\Micr...	rundll32.exe oobefldr.dll,ShowWelcomeCen...
C:\Windows\system32\mshta.exe "%1"...	\REGISTRY\MACHINE\SOFTWARE\Classes...	C:\Windows\system32\mshta.exe "%1" %*
SilkTest Agent	\REGISTRY\MACHINE\SOFTWARE\Microso...	"C:\Automation\startagent.bat"
AVG_TRAY	\REGISTRY\MACHINE\SOFTWARE\Microso...	C:\Program Files\AVG\AVG10\avgtray.exe
VMware User Process	\REGISTRY\MACHINE\SOFTWARE\Microso...	"C:\Program Files\VMware\VMware Tools\V...
Sidebar	\REGISTRY\USER\S-1-5-21-2323238519-...	C:\Program Files\Windows Sidebar\sidebar.e...
SHELL	\INI\system.ini\BOOT\SHELL	SYS:Microsoft\Windows NT\CurrentVersion...
VMware Tools	\REGISTRY\MACHINE\SOFTWARE\Microso...	"C:\Program Files\VMware\VMware Tools\V...
hffsrsv	\REGISTRY\MACHINE\SOFTWARE\Microso...	c:\windows\hffext\hffsrsv.exe
Adobe Reader Speed Launcher	\REGISTRY\MACHINE\SOFTWARE\Microso...	"C:\Program Files\Adobe\Reader 8.0\Reade...
Sidebar	\REGISTRY\USER\S-1-5-19\Software\Micr...	%ProgramFiles%\Windows Sidebar\Sidebar...
Applnit_DLLs	\REGISTRY\MACHINE\SOFTWARE\Microso...	qaphooks.dll

At the bottom of the window, there are buttons for "Selectie verwijderen" (Remove selection) and "Terug" (Back). On the left side, there are buttons for "Overzicht" (Overview), "Systeemprogramma's" (System programs), "Nu scannen" (Scan now), "Scanopties" (Scan options), "Anti-Rootkitscan", and "Nu bijwerken" (Update now).

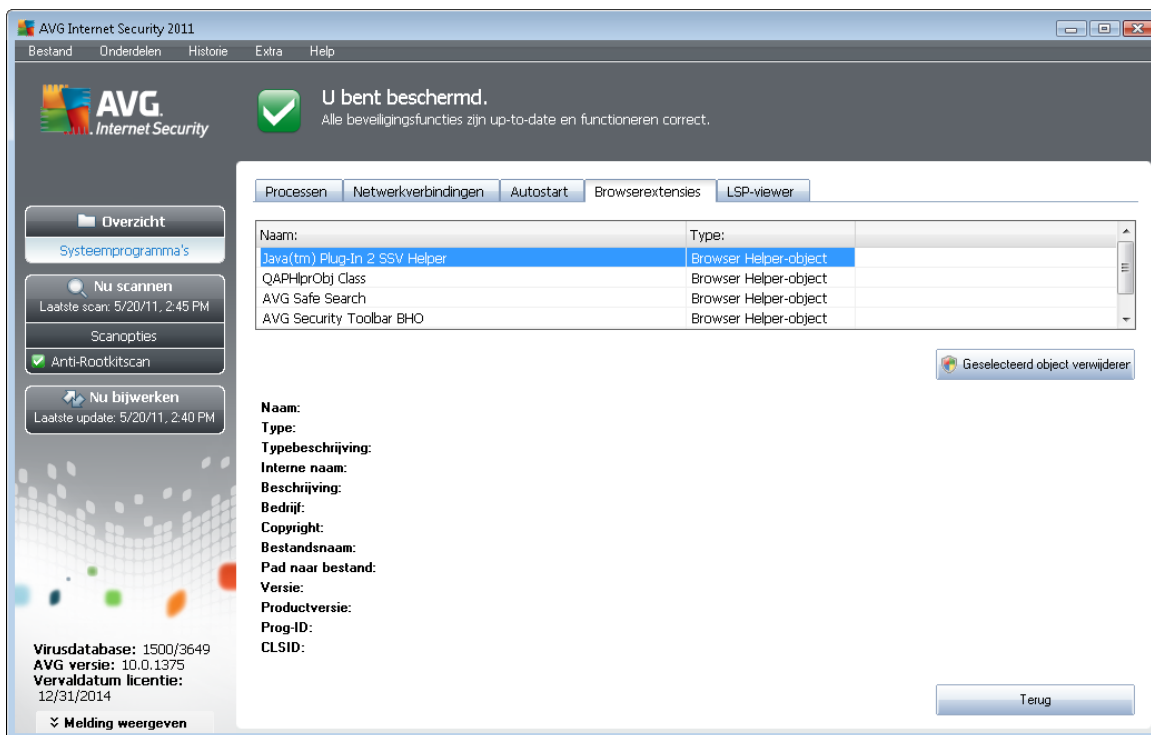
In het dialoogvenster **Autostart** staat een lijst met alle toepassingen die worden gestart bij het opstarten van Windows. Vaak voegen meerdere malware-toepassingen zichzelf automatisch toe aan het item in het opstartregister.

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



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

7.15.4. Browserextensies



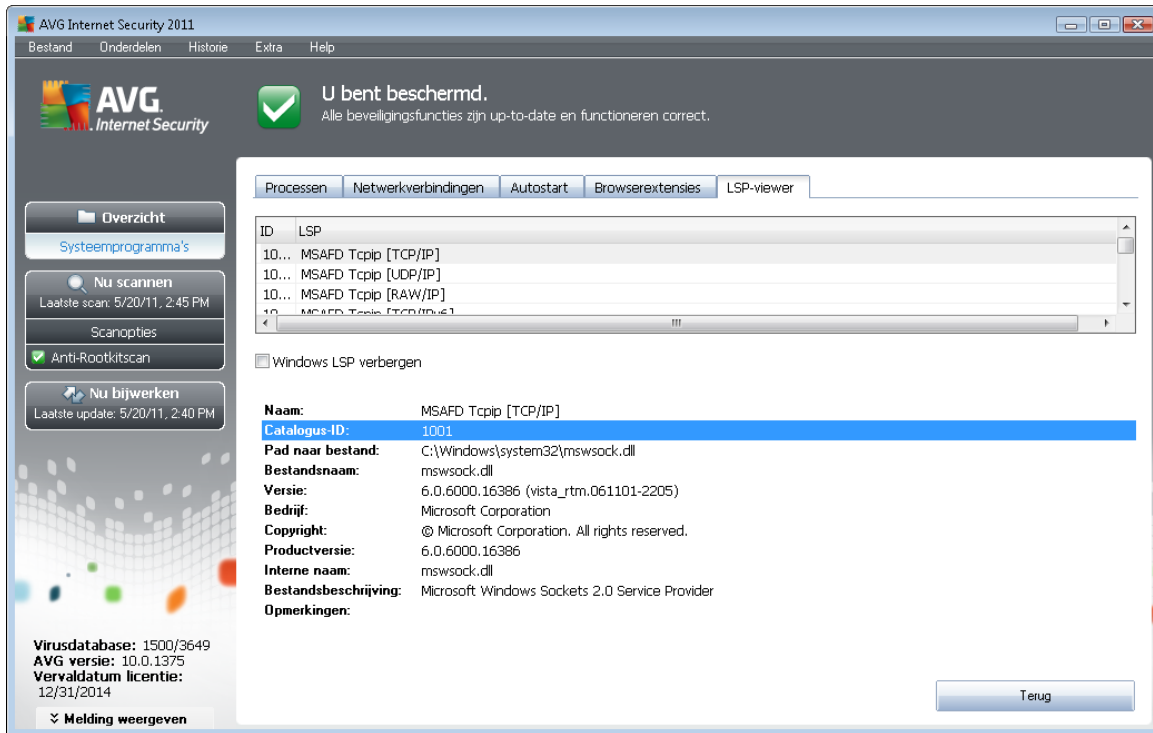
In het dialoogvenster **Browserextensies** staat een lijst met invoegtoepassingen (, *dat wil zeggen toepassingen*) die zijn geïnstalleerd in uw internetbrowser. Deze lijst kan invoegtoepassingen bevatten voor reguliere toepassingen maar ook potentiële malware-programma's. Klik op een object in de lijst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

Knoppen

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

- **Geselecteerd object verwijderen** - de op dat moment in de lijst geselecteerde invoegtoepassing verwijderen. **Het verwijderen van invoegtoepassingen uit de lijst raden we u ten zeerste af, tenzij u absoluut zeker weet dat deze een reële bedreiging vormen!**
- **Terug** - als u op deze knop klikt, keert u terug naar de standaard [AVG-gebruikersinterface](#) (Overzicht van onderdelen)

7.15.5. LSP-viewer



In het dialogvenster **LSP Viewer** staat een lijst met Layered Service Providers (LSP).

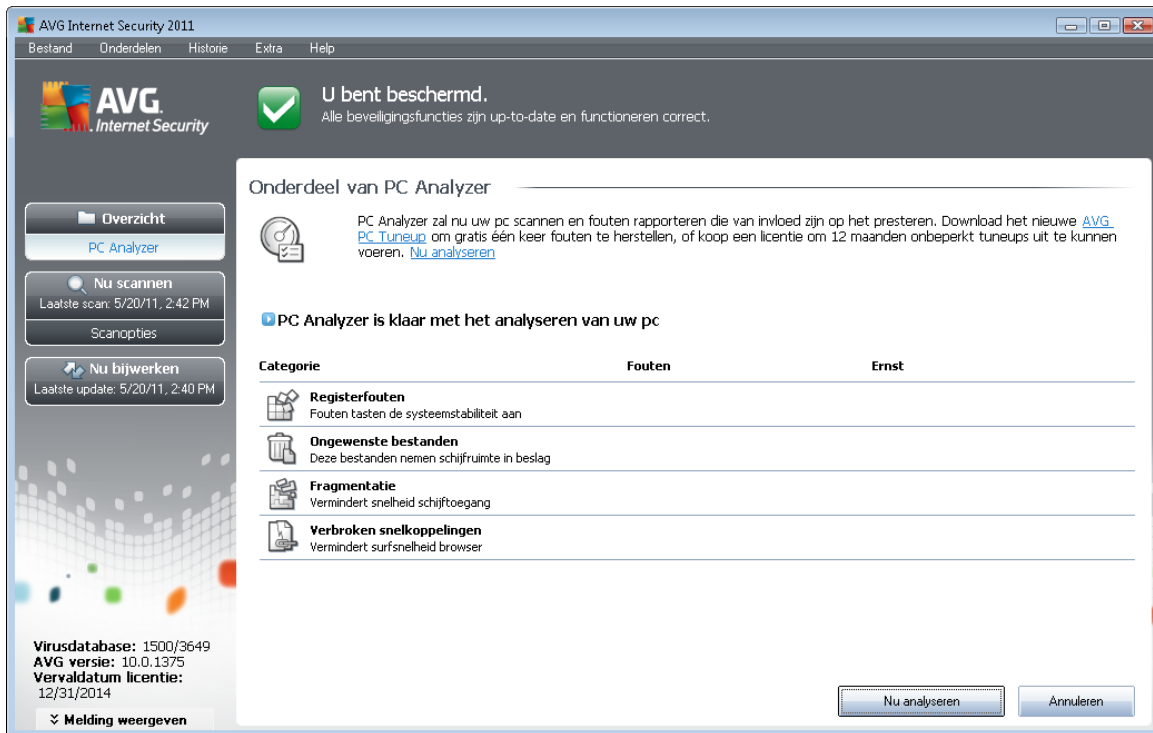
Een **Layered Service Provider** (LSP) is een systeemstuurprogramma dat is gekoppeld aan de netwerkservices van het Windows-besturingssysteem. Het verschaft toegang tot alle gegevens die de computer binnenkomen en verlaten, en kan deze gegevens ook wijzigen. Sommige LSP's zijn nodig om Windows een verbinding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

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

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

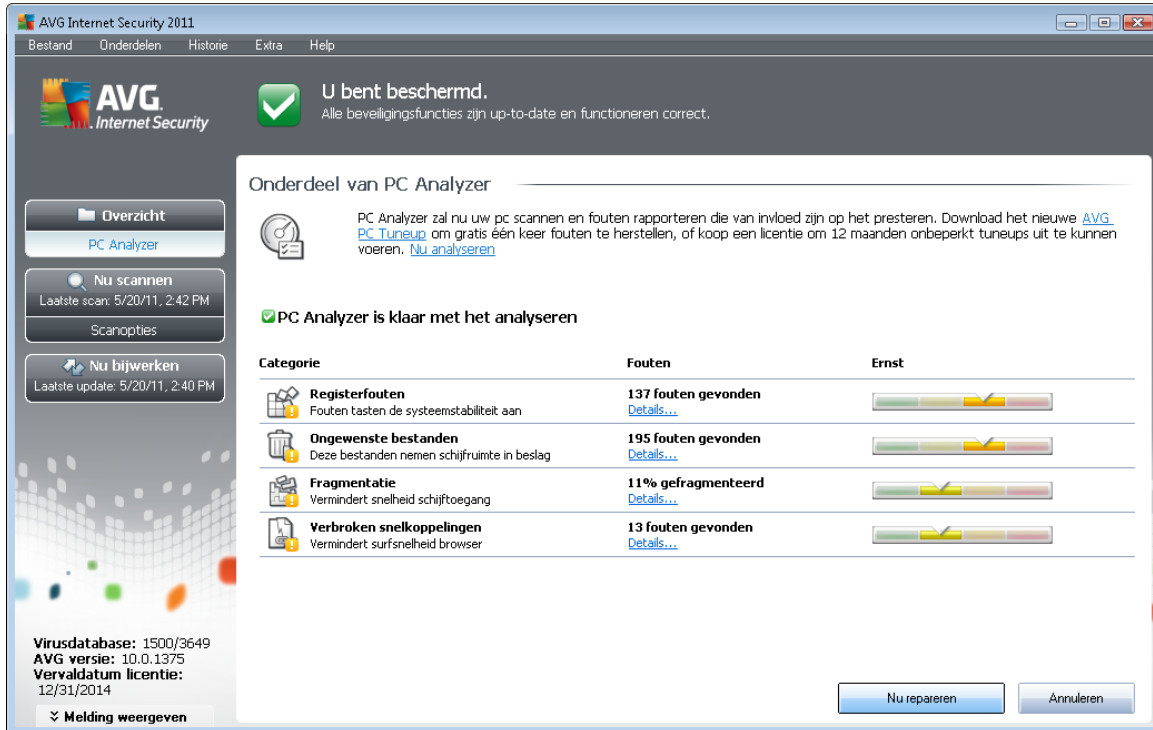
7.16. PC Analyzer

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** – het percentage van de vaste schijf dat is gefragmenteerd, dat wil zeggen al lange tijd in gebruik is, zodat de meeste bestanden in delen zijn opgeslagen op verschillende plaatsen op 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:



U bent beschermd.
Alle beveiligingsfuncties zijn up-to-date en functioneren correct.

Onderdeel van PC Analyzer

PC Analyzer zal nu uw pc scannen en fouten rapporteren die van invloed zijn op het presteren. Download het nieuwe [AVG PC Tuneup](#) om gratis één keer fouten te herstellen, of koop een licentie om 12 maanden onbeperkt tuneups uit te kunnen voeren. [Nu analyseren](#)

PC Analyzer is klaar met het analyseren

Categorie	Fouten	Ernst
Registerfouten Fouten tasten de systeemstabiliteit aan	137 fouten gevonden Details...	
Ongewenste bestanden Deze bestanden nemen schijfruimte in beslag	195 fouten gevonden Details...	
Fragmentatie Vermindert snelheid schijftoegang	11% gefragmenteerd Details...	
Verbroken snelkoppelingen Vermindert surfsnelheid browser	13 fouten gevonden Details...	

Virusdatabase: 1500/3649
AVG versie: 10.0.1375
Vervaldatum licentie: 12/31/2014

Melding weergeven

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) – de website van AVG (<% [AVG website](#)%>), in het bijzonder de pagina met gedetailleerde en actuele informatie over het onderdeel **PC Analyzer** wordt weergegeven
- **Annuleren** – afbreken van de analyse die wordt uitgevoerd, terugkeren naar de standaard [gebruikersinterface van AVG](#) (het onderdelenoverzicht) na voltooiing van de analyse

7.17. ID Protection

AVG Identity Protection is een anti-malwareproduct dat zich richt op preventie van diefstal van uw wachtwoorden, bankrekeninggegevens, creditcardnummers en andere persoonlijke digitale waardevolle informatie door allerlei vormen van schadelijke software (*malware*) die uw pc bedreigen. Het product controleert of alle programma's die worden uitgevoerd op uw pc correct functioneren.

AVG Identity Protection werkt door doorlopend verdacht gedrag te detecteren en te blokkeren en beschermt uw computer tegen alle nieuwe schadelijke software.

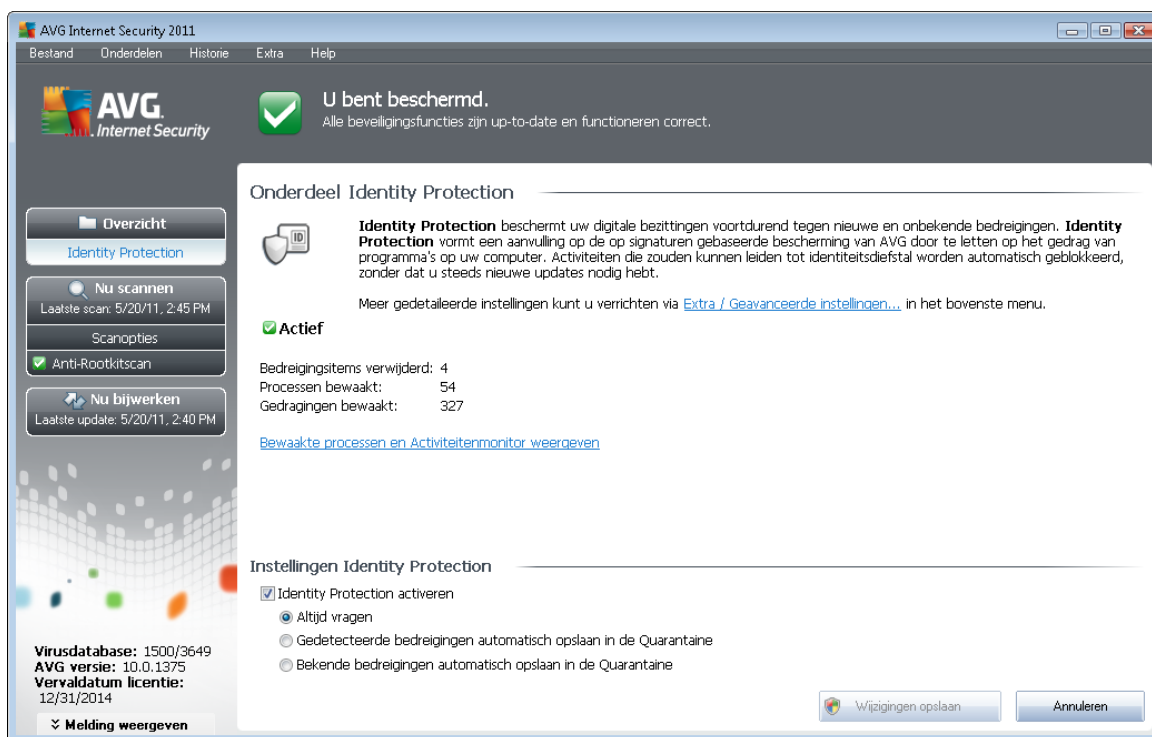


7.17.1. ID Protection principes

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

We raden u met nadruk aan om zowel [AVG Anti-Virus](#) als **AVG Identity Protection te installeren om uw pc volledig te beschermen.**

7.17.2. ID Protection interface



De interface van het onderdeel **Identity Protection** biedt een beknopt overzicht van de basisfunctionaliteit en de status van het onderdeel en enig cijfermateriaal:

- **Malware-items verwijderd** – het aantal toepassingen dat is gedetecteerd als malware en is verwijderd
- **Bewaakte processen** – het aantal toepassingen dat op dat moment wordt uitgevoerd en wordt bewaakt door IDP
- **Bewaakte gedragingen** – het aantal specifieke acties dat in de bewaakte toepassingen wordt uitgevoerd



Daaronder staat de koppeling [Bewaakte processen en activiteitenmonitor weergeven](#) waarmee u de gebruikersinterface van het onderdeel [Systeemprogramma's](#) opent, waarin een gedetailleerd overzicht wordt gegeven van alle bewaakte processen.

Instellingen Identity Protection

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

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

Het kan voorkomen dat **Identity Protection** een legitiem bestand als verdacht of gevaarlijk rapporteert. Aangezien **Identity Protection** bedreigingen herkent op grond van hun gedrag, treedt dit probleem meestal op wanneer een programma toetsaanslagen opslaat of andere programma's installeert, of wanneer er een nieuw stuurprogramma op de computer wordt geïnstalleerd. Maak daarom een keuze uit één van de volgende manieren waarop **Identity Protection** kan reageren als er verdachte activiteiten worden gedetecteerd:

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

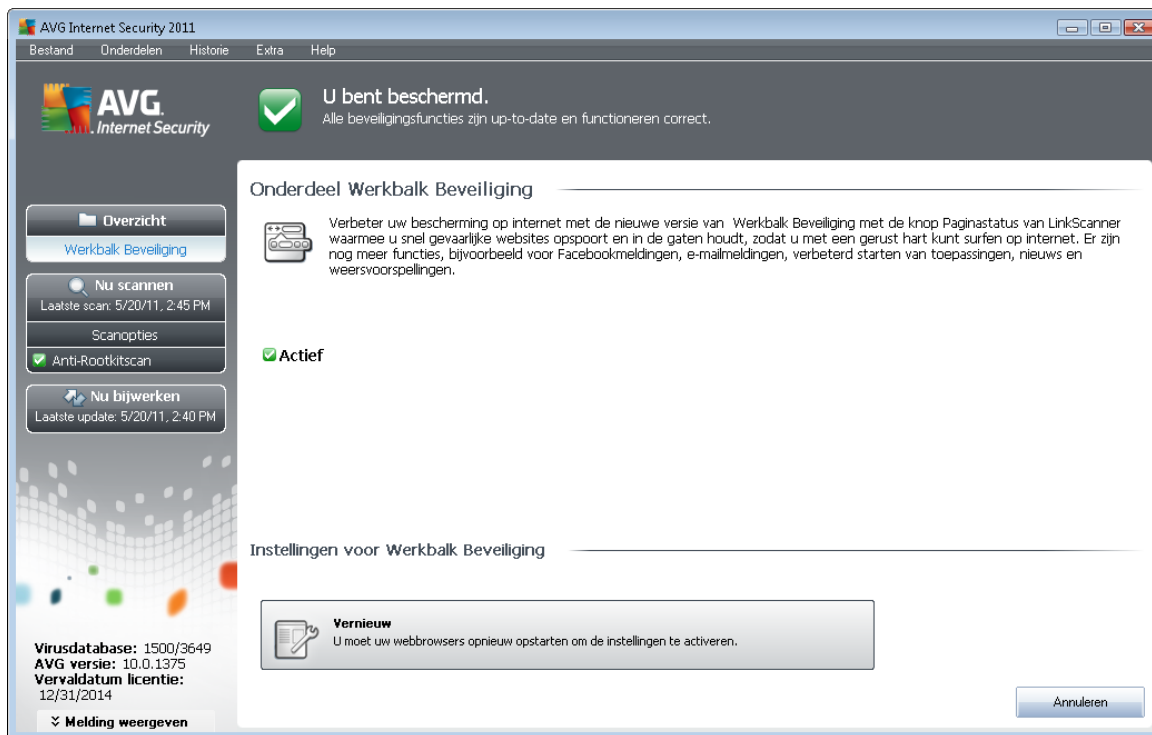
Knoppen

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

- **Wijzigingen opslaan** – klik op deze knop om de wijzigingen die u in het dialoogvenster hebt aangebracht op te slaan en toe te passen
- **Annuleren** – terugkeren naar de standaard [AVG-gebruikersinterface](#) (*het overzicht van onderdelen*)

7.18. Werkbalk Beveiliging

De **Werkbalk Beveiliging** is een optionele webbrowserwerkbalk, die betere AVG-bescherming biedt, naast verschillende functies die u terzijde staan als u op internet surft. De **Werkbalk Beveiliging** wordt ondersteund door Internet Explorer (6.0 en hoger) en Mozilla Firefox (3.0 en hoger):



Alle instellingen van het onderdeel **Werkbalk Beveiliging** zijn direct toegankelijk vanaf de [Werkbalk Beveiliging](#) in de webbrowser.



8. AVG Werkbalk Beveiliging

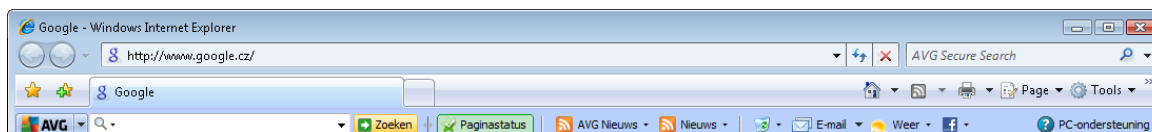
AVG Werkbalk Beveiliging is een nieuwe tool die samenwerkt met het onderdeel [LinkScanner](#). De **AVG Werkbalk Beveiliging** kan worden gebruikt voor het aansturen van de functies van [LinkScanner](#) en het aanpassen van het gedrag van dat onderdeel.

Als u ervoor kiest om de werkbalk te installeren tijdens de installatie van **AVG Internet Security 2011**, wordt de werkbalk automatisch toegevoegd aan uw webbrowser (*Internet Explorer 6.0 of hoger, en Mozilla Firefox 3.0 of hoger*). Andere internetbrowsers worden op dit moment niet ondersteund.

Opmerking: als u een andere browser gebruikt (bijvoorbeeld de Avant browser) kan er onverwacht gedrag optreden.

8.1. Interface van de AVG Werkbalk Beveiliging

De **AVG Werkbalk Beveiliging** is ontwikkeld voor samenwerking met **MS Internet Explorer** (versie 6.0 of hoger) en **Mozilla Firefox** (versie 3.0 of hoger). Als u eenmaal hebt besloten dat u de **Werkbalk Beveiliging** wilt installeren (tijdens het [installatieproces van AVG](#) is u gevraagd of u het onderdeel wel of niet wilde installeren), wordt het onderdeel in de webbrowser meteen onder de adresbalk geplaatst:



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

8.1.1. Knop AVG-logo

Deze knop biedt toegang tot algemene items van de werkbalk. Klik op de logoknop om naar de [website van AVG](#) te gaan. Klikt u op het pijltje naast het AVG-logo, dan wordt een menu geopend met de volgende items:

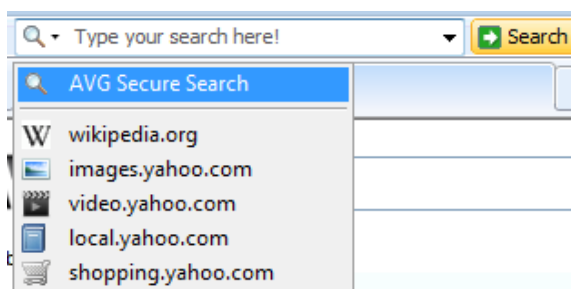
- **Werkbalkinfo** – een koppeling naar de introductiepagina van de **AVG Werkbalk Beveiliging** met aanvullende informatie over de bescherming die de werkbalk biedt
- **AVG starten** – de gebruikersinterface openen van **AVG Internet Security 2011** [AVG](#)
- **AVG Info** – er wordt een snelmenu geopend met de volgende koppelingen naar belangrijke beveiligingsinformatie met betrekking tot **AVG Internet Security 2011**:
 - *Over bedreigingen* – De [website van AVG](#) wordt geopend op de pagina met de belangrijkste informatie over de grootste bedreigingen, aanbevelingen voor het verwijderen van virussen, informatie over AVG-updates, toegang tot de [Virusdatabase](#) en nog meer relevante informatie
 - *AVG-nieuws* – de webpagina met het meest recente persbericht over AVG wordt geopend

- *Huidig bedreigingsniveau* – de webpagina van het viruslab wordt geopend met een grafische weergave van het huidige bedreigingsniveau op internet
- *AVG Threat Labs* – de website [AVG Site Reports](#) wordt geopend, waarop u op naam kunt zoeken naar gedetailleerde informatie over specifieke bedreigingen
- **Opties** – er wordt een configuratiedialogvenster geopend waarin u de instellingen voor de **AVG Werkbalk Beveiliging** naar wens kunt aanpassen – zie het volgende hoofdstuk [AVG Werkbalk Beveiliging Opties](#)
- **Geschiedenis wissen** – wissen via de **AVG Werkbalk Beveiliging** van de volledige historie, of afzonderlijk de zoekhistorie, browserhistorie, downloadhistorie en cookies.
- **Update** – controleren of er nieuwe updates beschikbaar zijn voor de **AVG Werkbalk Beveiliging**
- **Help** – opties voor het openen van het Help-bestand, het opnemen van contact met de [technische ondersteuning van AVG](#) en de weergave van details van de huidige versie van de werkbalk

8.1.2. Zoekvak van AVG Secure Search (powered by Google)

AVG Secure Search (powered by Google) het zoekvak is een eenvoudige en veilige functie om op internet te zoeken met AVG Secure Search (powered by Google). Typ een trefwoord of een paar woorden in het zoekvak en klik op de knop **Zoeken**, of druk op de toets **Enter** om meteen de zoekopdracht uit te voeren met de zoekmachine van AVG Secure Search (powered by Google), ongeacht welke pagina op dat moment wordt weergegeven. Aan het zoekvak is bovendien een keuzelijst gekoppeld met eerdere zoekopdrachten. De resultaten van zoekopdrachten die u via dit zoekvak opgeeft, worden geanalyseerd met [Search-Shield](#).

U kunt in het zoekvak ook overschakelen naar Wikipedia, of een andere zoekservice – zie de afbeelding:







8.1.3. Paginastatus

Deze knop toont direct op de werkbalk het oordeel over de op dat moment weergegeven pagina, gebaseerd op criteria van het onderdeel [Surf-Shield](#):

-  – De gekoppelde pagina is veilig



-  – pagina is enigszins verdacht.
-  – er staan koppelingen op de pagina naar gevaarlijke pagina's.
-  – 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.

Klik op de knop om een informatievenster te openen dat gedetailleerde gegevens bevat over de specifieke webpagina.

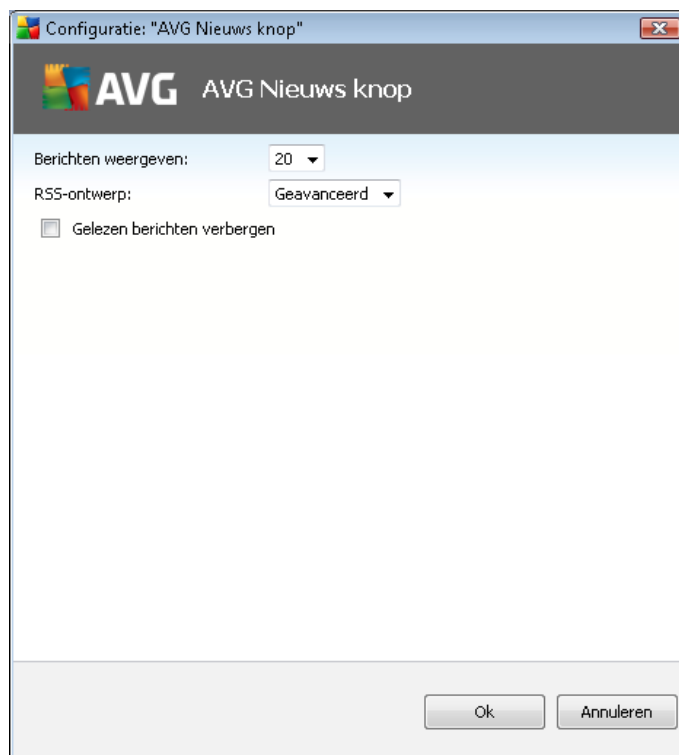
8.1.4. AVG Nieuws


Direct vanaf de **AVG Werkbalk Beveiliging** opent u met deze knop een overzicht van de laatste **nieuwsberichten** met betrekking tot AVG, zowel artikelen uit de media als persberichten van het bedrijf zelf:



In de rechterbovenhoek staan twee knoppen:

-  – met deze knop opent u het dialoogvenster waarin u parameters kunt opgeven voor de knop **AVG Nieuws** die op de **AVG Werkbalk Beveiliging** staat:




- **Berichten weergeven** – het aantal berichten wijzigen dat in één keer wordt weergegeven
- **RSS design** – kiezen tussen een geavanceerde modus en een basismodus voor de huidige weergave van het nieuwsoverzicht (*standaard is de geavanceerde modus geselecteerd – zie bovenstaande afbeelding*)
- **Gelezen berichten verbergen** – als deze optie is ingeschakeld, worden gelezen berichten niet langer weergegeven, zodat ruimte ontstaat voor nieuwe berichten
-  – Met een klik op deze knop sluit u het op dat moment weergegeven nieuwsoverzicht

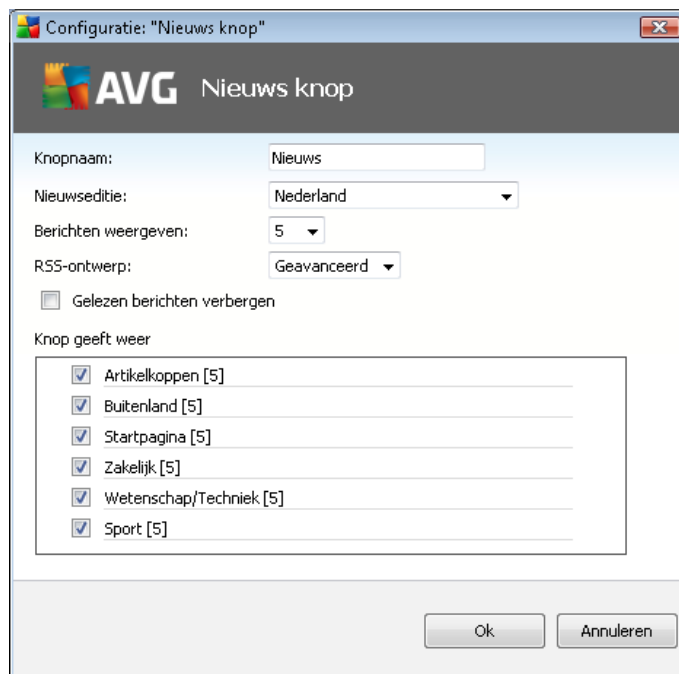
8.1.5. Nieuws

Op vergelijkbare manier kunt u met deze knop vanaf de **AVG Werkbalk Beveiliging** een overzicht oproepen van het laatste nieuws gepresenteerd door diverse media, verdeeld in categorieën:




In de rechterbovenhoek staan twee knoppen:

-  – het dialoogvenster openen waarin u parameters kunt opgeven voor de knop **Nieuws** die op de **AVG Werkbalk Beveiliging** staat:



- **Knopnaam** – u kunt de knopnaam wijzigen die wordt weergegeven op de **AVG Werkbalk Beveiliging**
- **Nieuwseditie** – selecteer in de lijst een land van waaruit u het nieuws wilt weergeven
- **Berichten weergeven** – geef op hoeveel berichten tegelijkertijd moeten worden weergegeven
- **RSS-design** – overschakelen tussen de basisoptie en de geavanceerde optie voor de weergave

van het nieuwsoverzicht (*standaard is geavanceerd design ingeschakeld, zie bovenstaande afbeelding*)

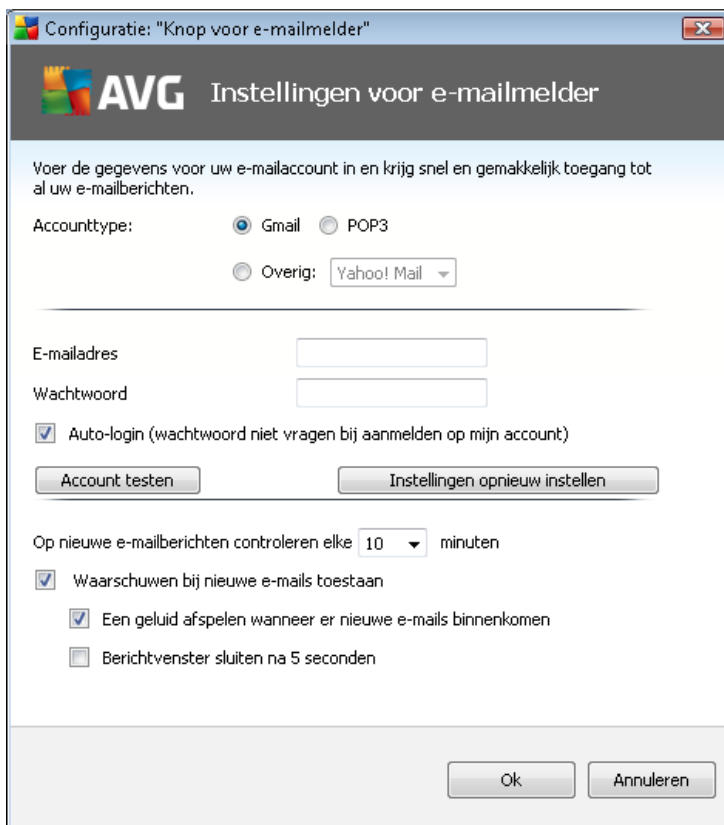
- **Verborgen berichten verbergen** – gelezen berichten moeten niet langer worden weergegeven in het nieuwsoverzicht om ruimte te maken voor nieuwe berichten
- **Weergave knop** – in dit veld kunt u opgeven wat voor soort nieuws moet worden weergegeven met het **nieuwsoverzicht van de AVG Werkbalk Beveiliging**
 -  – Met een klik op deze knop sluit u het op dat moment weergegeven nieuwsoverzicht

8.1.6. Historie wissen

Met deze knop kunt u de browsergeschiedenis wissen op dezelfde manier als met de optie **AVG-Logo -> Historie wissen**.

8.1.7. E-mailmelding

Met de knop **E-mailmelding** kunt u de functie inschakelen die u direct waarschuwt op de [AVG Werkbalk Beveiliging](#) wanneer er een nieuwe e-mail binnenkomt. Met de knop opent u het volgende dialoogvenster waarin u parameters kunt opgeven voor uw e-mailaccount en de regels voor weergave van e-mail. Volg de instructies in het dialoogvenster:



- **Accounttype** – Geef op van welk protocol uw e-mailaccount gebruikmaakt. U kunt kiezen uit de volgende mogelijkheden: *Gmail*, *POP3*, of een servernaam uit de vervolgkeuzelijst bij *Overig* (op dit moment kunt u daar kiezen uit *Yahoo! JP Mail of Hotmail* Als u niet precies weet van welk servertype uw e-mailaccount gebruikmaakt, probeert u dat te achterhalen via uw mailprovider of uw internetserviceprovider.

- **Aanmelden** – geef exact uw *e-mailadres* op, en het bijbehorende *wachtwoord*. Handhaaf de selectie van de optie *Automatisch aanmelden* zodat u de gegevens niet steeds opnieuw hoeft op te geven.
- **Account testen** – klik op deze knop om de ingevoerde gegevens te testen.
- **Instellingen opnieuw instellen** – in één keer de ingevoerde gegevens wissen.
- **Op nieuwe e-mail controleren om de ... minuten** – geef het tijdsinterval op waarmee op nieuwe e-mail moet worden gecontroleerd (*in een bereik van 5-120 minuten*) en geef op hoe u wilt worden gewaarschuwd dat er nieuwe e-mail is.
- **Nieuwe e-mailwaarschuwingen toestaan** - schakel dit selectievakje uit als u geen berichtvenster wilt weergeven bij nieuwe e-mail.
 - **Een geluid afspelen bij nieuwe e-mail** – schakel dit selectievakje uit als u geen geluidswaarschuwingen wilt bij nieuwe e-mail.
 - **Berichtvenster sluiten na 5 seconden** – schakel dit selectievakje in als u het berichtvenster bij nieuwe e-mail na 5 seconden weer wilt sluiten.

8.1.8. Weerinfo

Met de knop **Weerinfo** geeft u informatie weer over de huidige temperatuur (*elke 3 tot 6 uur bijgewerkt*) op de locatie die u in de interface van de **AVG Werkbalk Beveiliging** hebt geselecteerd. Klik op de knop om een infopaneel te openen met een gedetailleerd weeroverzicht:



Brno, CZ °F °C
 [[Locatie wijzigen](#)]

 **25° C**
 Windsnelheid: 16,09 km/h
 Zonsopkomst: 05:04
 Zonsondergang: 20:34

 <p>vr Hoog: 24 °C Laag: 14 °C</p>	 <p>za Hoog: 25 °C Laag: 14 °C</p>
---	---

Bijgewerkt 05/20/2011 13:42:34 **YAHOO! NEWS** [Volledige vooruitzichten >](#)

U hebt de volgende opties:

- **Locatie wijzigen** – klik op de knop **Locatie wijzigen** om een dialoogvenster **Locatie zoeken** te openen. Voer de naam in van de gewenste locatie in het tekstveld en bevestig de zoekopdracht door te klikken op de knop **Zoeken**. Selecteer in de lijst met locaties die dezelfde naam hebben, de door u gewenste locatie. Tot slot wordt dan het infopaneel met



het weeroverzicht van de door u geselecteerde locatie weergegeven.

- **Fahrenheit-Celsiusconverter** – in de rechterbovenhoek van het infopaneel kunt u kiezen uit temperatuurmeting in Fahrenheit en Celsius. Op basis van uw keuze wordt daarna de temperatuur aangegeven.
- **Volledige voorspelling** – klik op de koppeling **Volledige voorspelling** als u geïnteresseerd bent in een uitgebreid weerbericht van de website.

8.1.9. Facebook

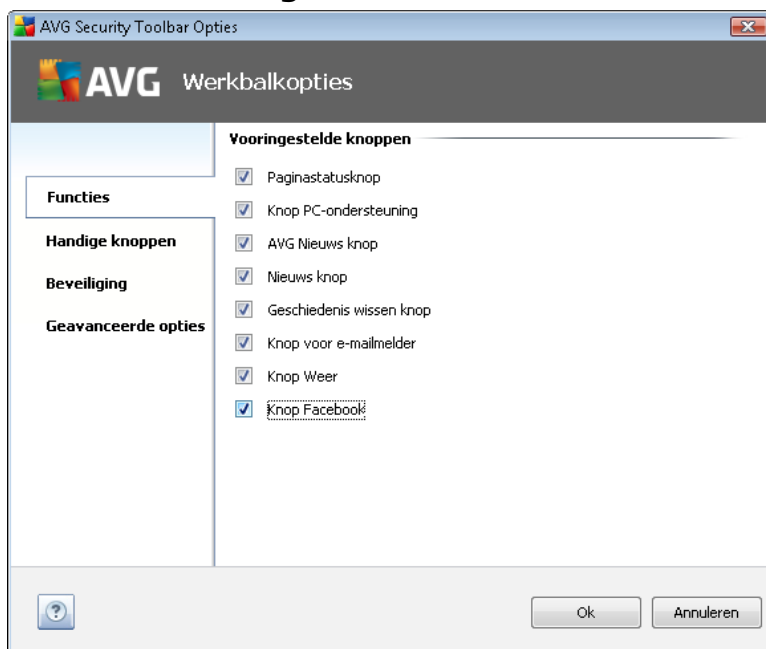
Met de knop **Facebook** kunt u verbinding maken met het sociale netwerk [Facebook](#), direct vanaf de **AVG Werkbalk Beveiliging**. Als u op de knop klikt, wordt de vraag weergegeven of u zich wilt aanmelden; klikt u er nogmaals op, dan wordt het **Facebook-aanmeldingsvenster** geopend. Voer uw aanmeldingsgegevens in en klik op de knop **Verbinden**. Als u nog geen [Facebook](#)account hebt, kunt u dat maken met behulp van de koppeling **Registreren bij Facebook**.

Zodra u het registratieproces voor [Facebook](#) hebt voltooid, wordt uw toestemming gevraagd voor installatie van de toepassing **AVG Social Extension**. De functionaliteit van die toepassing is van essentieel belang voor de verbinding tussen de werkbalk en [Facebook](#); we raden u dan ook aan de installatie toe te staan. Na installatie wordt de [Facebook](#)-verbinding geactiveerd en functioneert de knop **Facebook** op de **AVG Werkbalk Beveiliging** als koppeling naar de standaardmenuopties van [Facebook](#).

8.2. AVG Werkbalk Beveiliging opties

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

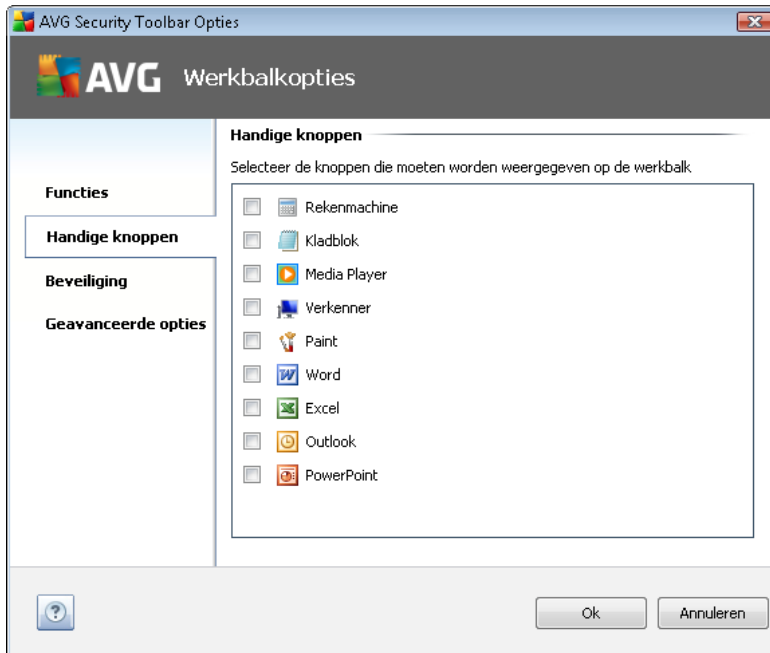
8.2.1. Tabblad Algemeen



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

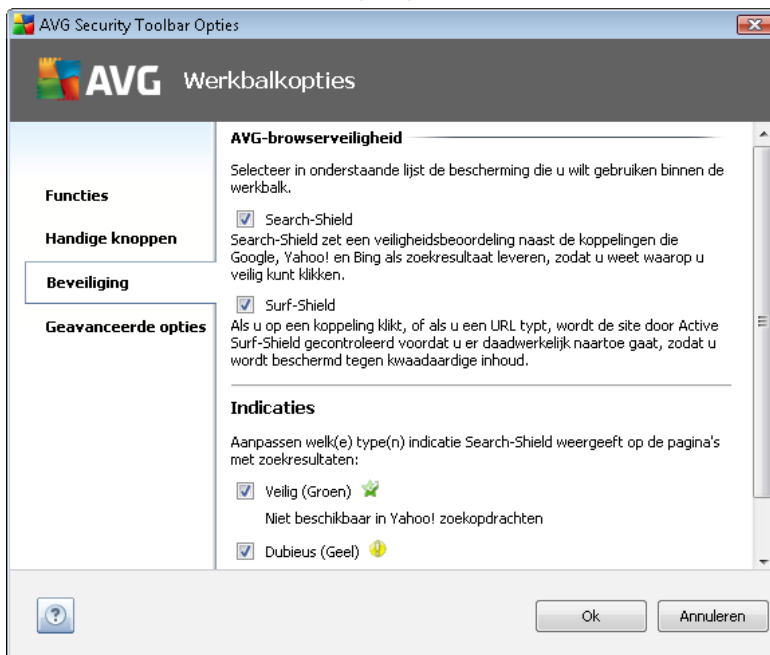
- **Knop *Paginastatus*** – weergave van de beveiligingsstatus van de op dat moment geopende pagina op de **AVG Werkbalk Beveiliging**
- **Knop *AVG-Nieuws*** – weergave van een webpagina met het meest recente persbericht over AVG
- **Knop *Nieuws*** – weergave van een gestructureerd overzicht van het dagelijkse nieuws
- **Knop *Historie wissen*** – volledige historie wissen, of de zoekgeschiedenis verwijderen, de browsergeschiedenis verwijderen, de downloadgeschiedenis verwijderen, of Cookies verwijderen, direct vanaf de AVG Werkbalk Beveiliging
- **Knop *E-mailmelding*** – melding van nieuw binnenkomende e-mailberichten op de **AVG Werkbalk Beveiliging**
- **Knop *Weer*** – weergave van informatie over de weerssituatie op een bepaalde locatie
- **Knop *Facebook*** – directe verbinding met het sociale netwerk [Facebook](#)

8.2.2. Tabblad Handige knoppen



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






8.2.3. Tabblad Beveiliging



Het tabblad **Beveiliging** is verdeeld in twee secties, **AVG-browserveiligheid** en **Indicaties**, waar u

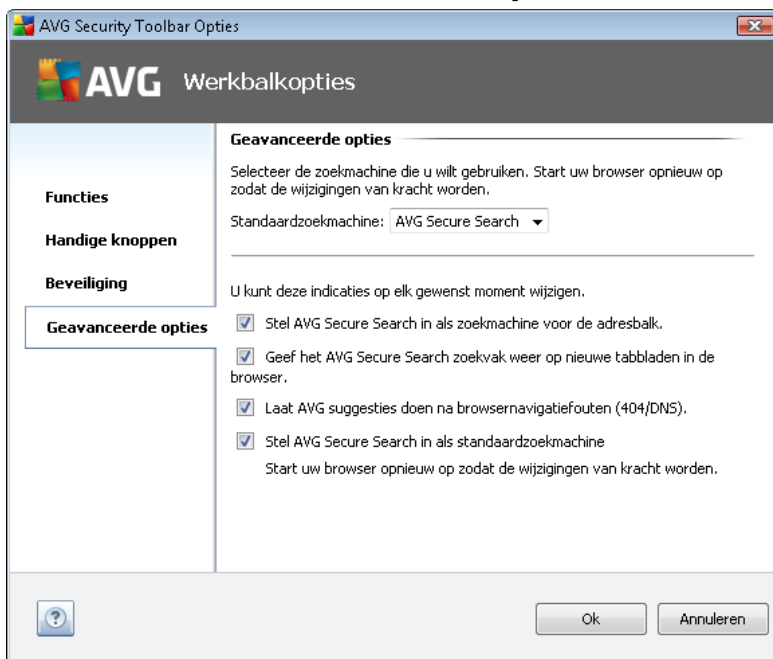


met behulp van selectievakjes kunt aangeven welke functionaliteit van de **AVG Werkbalk Beveiliging** u wilt gebruiken:

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

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

8.2.4. Tabblad Geavanceerde opties





Op het tabblad **Geavanceerde opties** selecteert u eerst de zoekmachine die u standaard wilt gebruiken. U kunt kiezen uit *AVG Secure Search (powered by Google)*, *Baidu*, *WebHledani*, *Yandex* en *Yahoo! JP*. Nadat u de standaardzoekmachine hebt gewijzigd, start u uw internetbrowser opnieuw op om de wijziging door te voeren.

U kunt er bovendien andere instellingen voor de **AVG Werkbalk Beveiliging** in- en uitschakelen (*wat wordt weergegeven verwijst naar de instellingen voor de standaard AVG Secure Search (powered by Google)*):

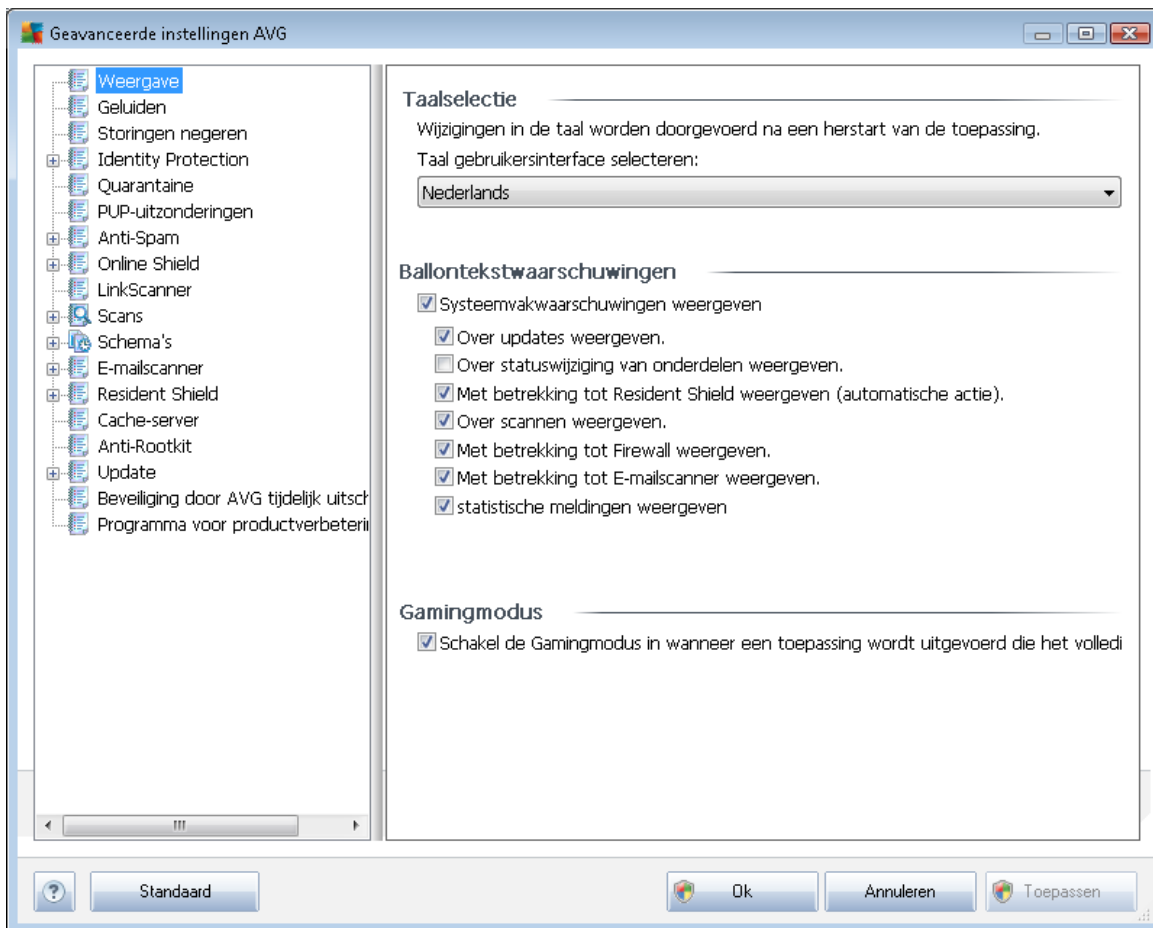
- **Stel AVG Secure Search (powered by Google) in als zoekmachine voor de adresbalk** – deze functie maakt het mogelijk om een trefwoord in te voeren op de adresbalk van de browser, waarmee Google vervolgens een zoekopdracht uitvoert naar relevante websites.
- **Laat AVG suggesties doen na browsernavigatiefouten (404/DNS)** – als u tijdens het zoeken op een niet-bestaande pagina terechtkomt, of op een pagina die niet kan worden weergegeven (404-fout), wordt er automatisch een webpagina weergegeven met daarop een overzicht van alternatieve pagina's die met het onderwerp verwant zijn en waaruit u kunt kiezen.
- **Stel AVG Secure Search (powered by Google) in als standaardzoekmachine** – Google is de standaardzoekmachine van de **AVG Werkbalk Beveiliging**; met deze optie maakt u Google ook tot standaardzoekmachine van de webbrowser.

9. AVG Geavanceerde instellingen

Het dialoogvenster voor een geavanceerde configuratie van **AVG Internet Security 2011** 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

De eerste optie in de navigatiestructuur in het linkerdeelvenster, **Weergave**, verwijst naar de algemene instellingen voor de [AVG-gebruikersinterface](#) en een paar basisinstellingen voor de manier waarop de toepassing werkt:

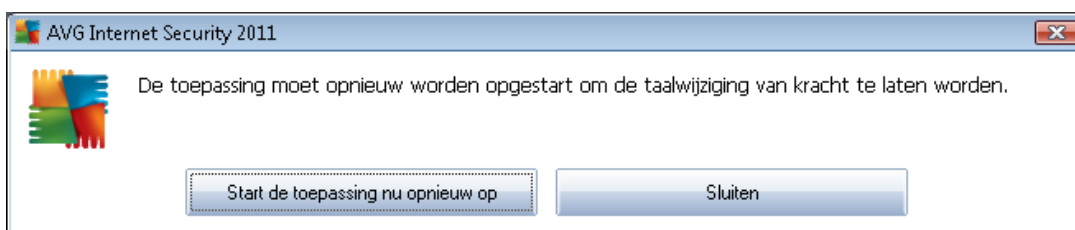


Taalselectie

In de sectie **Taalselectie** kunt u in de vervolgkeuzelijst een taal selecteren; die taal wordt dan overal in de [AVG Gebruikersinterface](#) toegepast. In de vervolgkeuzelijst staan alleen de talen die u hebt geselecteerd voor installatie bij de [installatie van het programma](#) (zie [Optie Aangepast](#)) en Engels (*wordt standaard geïnstalleerd*). Voor het voltooien van de procedure om over te stappen op een

andere taal, zult u de gebruikersinterface opnieuw moeten starten; ga als volgt te werk:

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



Ballontekstwaarschuwingen

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

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

- **Systeemwaarschuwingen weergeven** – standaard staat een vinkje bij deze optie (*ingeschakeld*) en worden Systeemvakmeldingen weergegeven. Schakel dit selectievakje uit als u in het geheel geen gebruik wilt maken van Systeemvakmeldingen. Als u de optie inschakelt, kunt u nader bepalen welke meldingen u wilt weergeven:
 - **Systeemvakmeldingen over updates** weergeven – maak een keuze of u meldingen van het starten, de voortgang en het voltooiën van de AVG-update wilt weergeven;
 - **Systeemvakmeldingen over statuswijziging van onderdelen weergeven** – maak een keuze of u informatie over de activiteit/inactiviteit van een onderdeel of mogelijk daarmee samenhangende problemen wilt weergeven. Bij het rapporteren van de foutstatus van een onderdeel, heeft deze optie hetzelfde effect als de informatieve functie van het [systeemvakpictogram](#) (kleurwijzigingen) waarmee een probleem wordt aangegeven met een onderdeel van AVG
 - **Systeemvakmeldingen met betrekking tot Resident Shield weergeven** – maak een keuze of u meldingen bij procedures voor het opslaan, kopiëren en openen van bestanden wilt weergeven of niet (*deze configuratie wordt alleen weergegeven als de optie [Automatisch herstel](#) in Resident Shield is geactiveerd*);
 - **Systeemvakmeldingen over scannen** weergeven – maak een keuze of u meldingen



van het automatisch starten van geplande scans, de voortgang en de resultaten wilt weergeven;

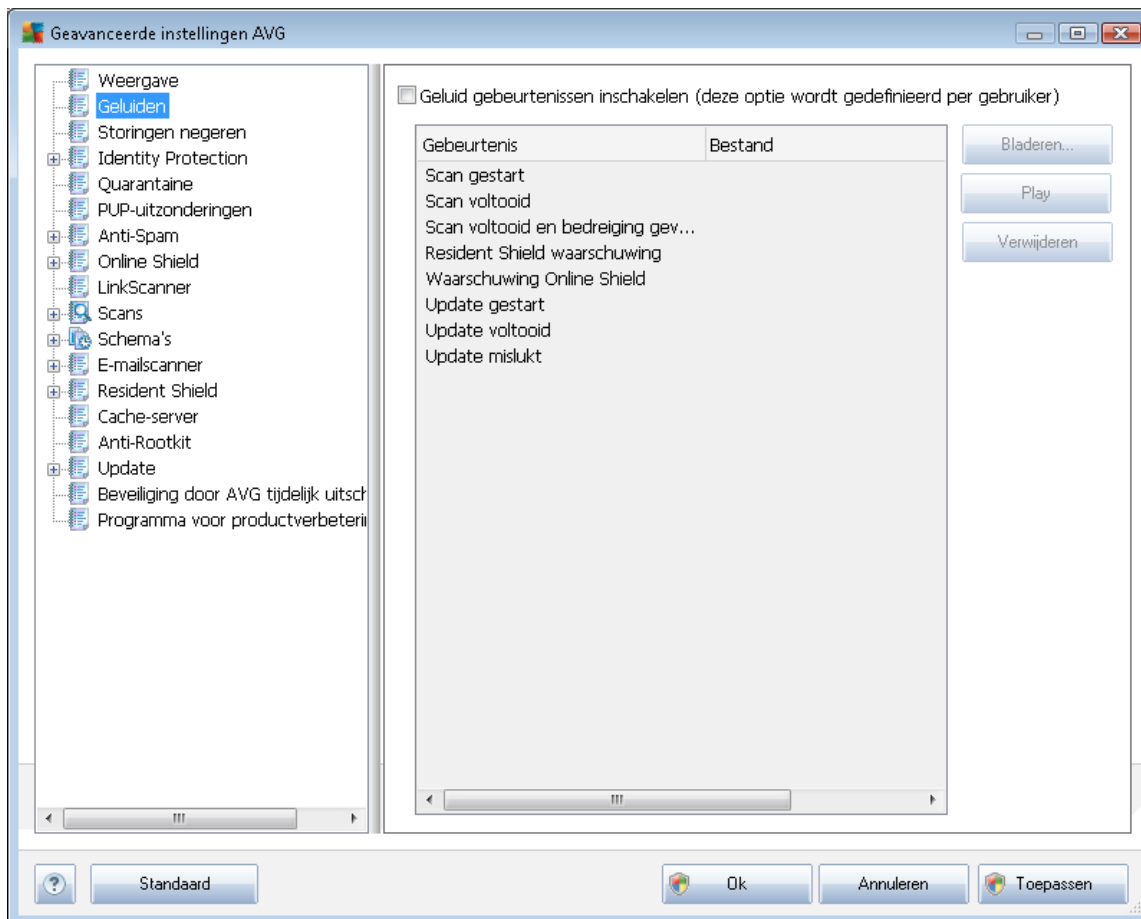
- **Systemvakmeldingen met betrekking tot Firewall weergeven** – maak een keuze of informatie over de status van Firewall en verwante processen, bijvoorbeeld waarschuwingen over het inschakelen/uitschakelen van het onderdeel, meldingen van geblokkeerd verkeer, enz., moet worden weergegeven;
- **Systemvakmeldingen met betrekking tot E-mailscanner weergeven** – maak een keuze of informatie over het scannen van alle binnenkomende en uitgaande e-mailberichten moet worden weergegeven.
- **Statistische meldingen weergeven** – regelmatig worden statistische gegevens weergegeven in het systeemvak als de optie is ingeschakeld.

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

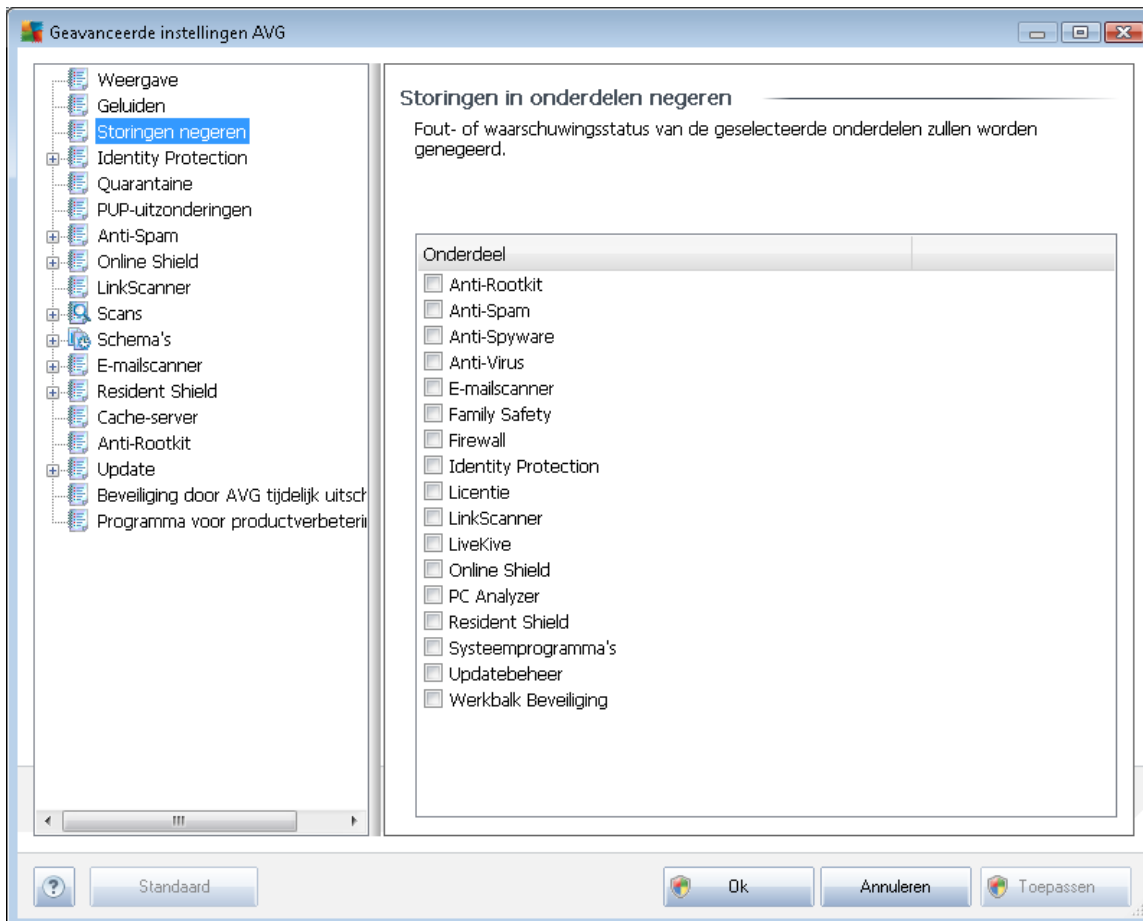


Selecteer dan een gebeurtenis in de lijst en zoek (**Bladeren**) op de vaste schijf een geluid dat u aan de gebeurtenis wilt toewijzen. Als u een voorbeeld van het geluid wilt afspelen, selecteert u de gebeurtenis in de lijst en klikt u op de knop **Afspelen**. Klik op de knop **Verwijderen** als u de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

Opmerking: alleen *.wav-geluiden worden ondersteund

9.3. Status negeren

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



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

- [systeemvakpictogram](#) – zolang alle onderdelen van AVG correct werken, wordt het pictogram weergegeven in vier kleuren; als er echter een fout optreedt, verschijnt er een geel uitroepteken in het pictogram,
- tekstbeschrijving van het huidige probleem in het gedeelte [Info Beveiligingsstatus](#) van het hoofdvenster van AVG.

Er zou zich een situatie kunnen voordoen waarin u een onderdeel tijdelijk moet uitschakelen (*Dit wordt niet aanbevolen. U zou moeten proberen alle onderdelen permanent ingeschakeld en in de standaardconfiguratie te houden, maar toch kan een dergelijke situatie zich voordoen*). In dat geval rapporteert het systeemvakpictogram automatisch de foutstatus van het onderdeel. In dit specifieke geval kan echter niet worden gesproken van een echte fout, omdat u deze opzettelijk hebt veroorzaakt en omdat u zich bewust bent van het potentiële risico. Tegelijkertijd kan het pictogram,



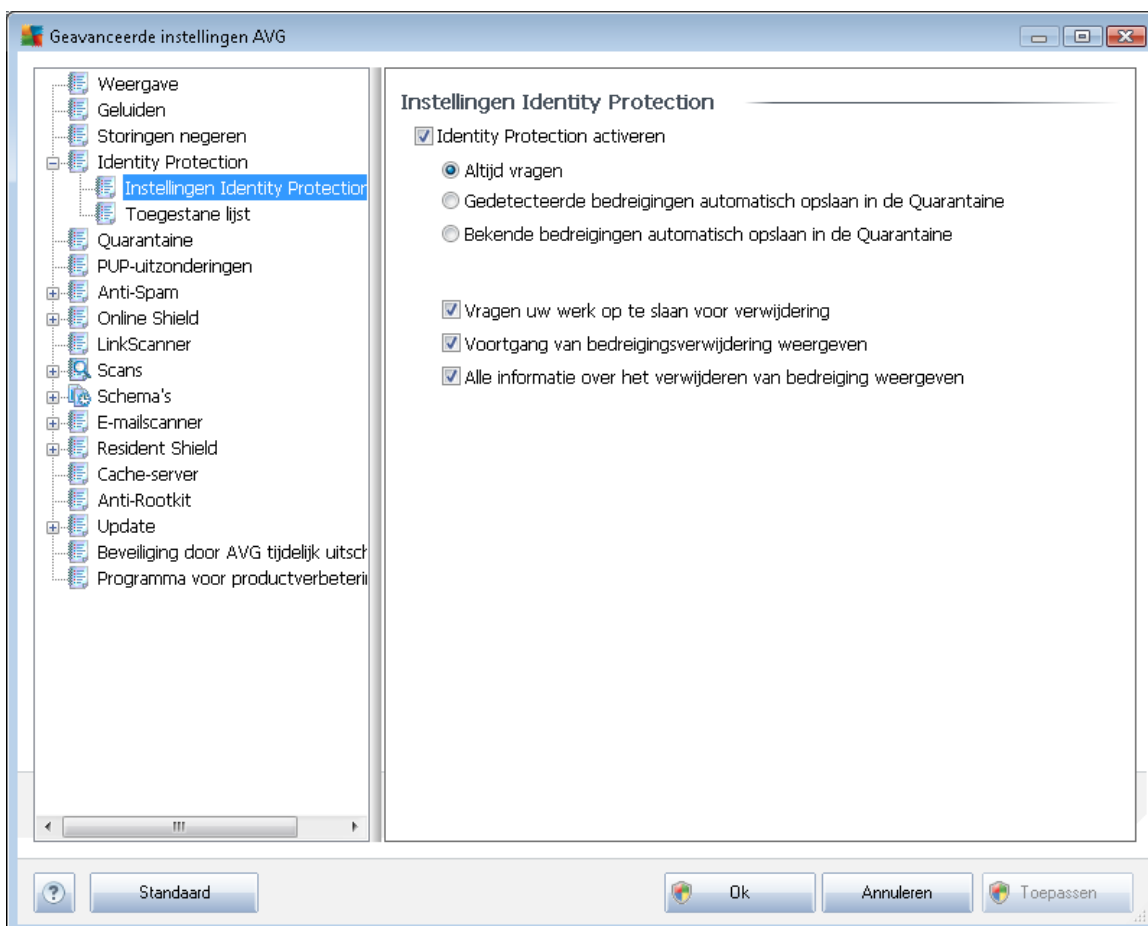
zodra dit grijs wordt weergegeven, niet eventuele echte fouten rapporteren die zich zouden kunnen voordoen.

Daarom kunt u in het dialoogvenster hierboven onderdelen selecteren die een foutstatus hebben (of die uitgeschakeld zijn) en waarover u niet wilt worden geïnformeerd. Voor specifieke onderdelen is dezelfde optie **Storingen in onderdelen negeren** ook beschikbaar rechtstreeks vanuit het [overzicht met onderdelen in het hoofdvenster van AVG](#).

9.4. Identity Protection

9.4.1. Identity Protection instellingen

In het dialoogvenster [Instellingen Identity Protection](#) kunt u de elementaire functies van het onderdeel [Identity Protection](#) in- en uitschakelen:



Identity Protection is actief (standaard ingeschakeld) – schakel dit selectievakje uit om het onderdeel [Identity Protection](#) uit te schakelen.

We raden u sterk aan dit alleen te doen als het beslist moet!



Als [Identity Protection](#) is ingeschakeld, kunt u opgeven wat er moet gebeuren als er een bedreiging wordt gedetecteerd:

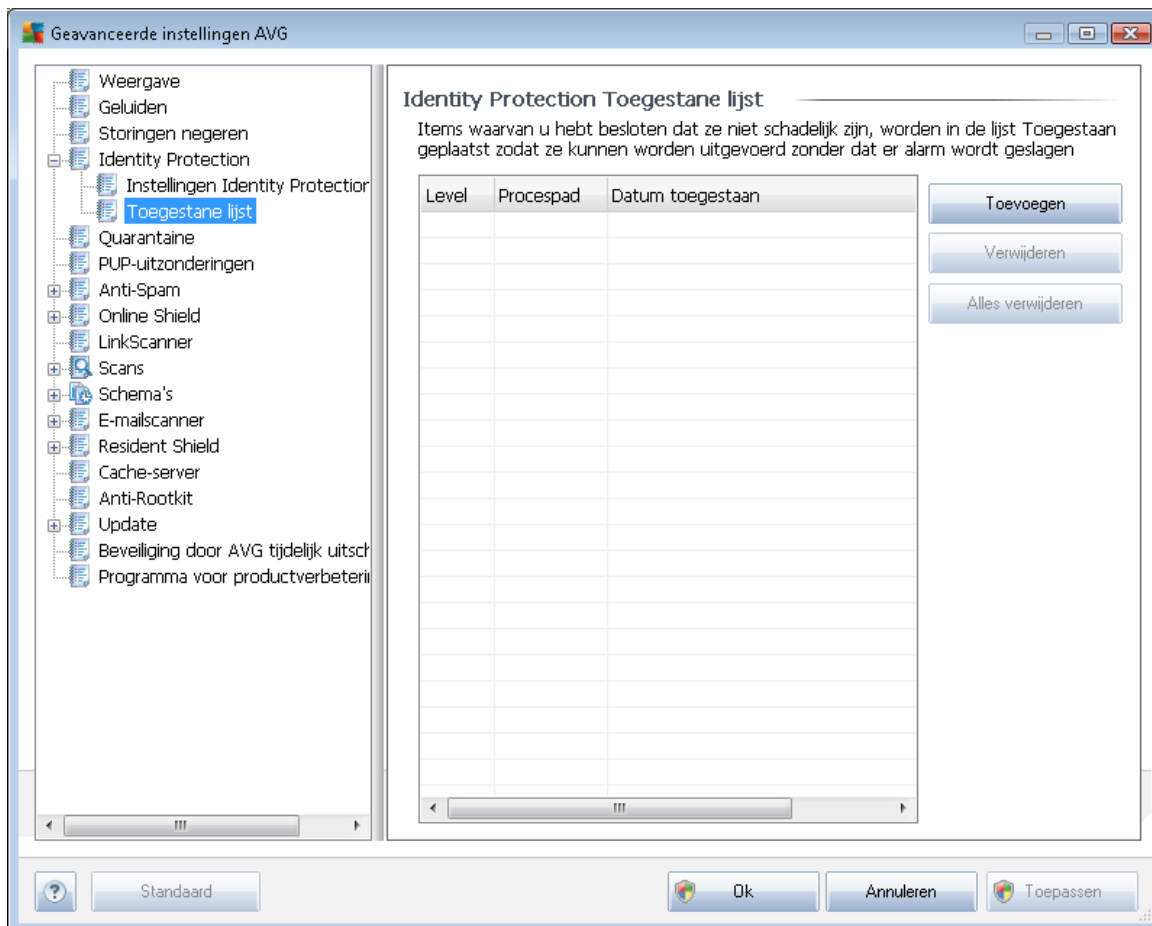
- **Altijd vragen** (*standaard ingeschakeld*) – bij detectie van een bedreiging wordt u gevraagd of deze naar de Quarantaine moet worden verplaatst, zodat u zeker weet dat er geen toepassingen die u wilt uitvoeren naar de Quarantaine worden verplaatst.
- **Gedetecteerde bedreigingen automatisch opslaan in de Quarantaine** – schakel dit selectievakje in als u wilt dat alle gedetecteerde mogelijke bedreigingen meteen worden verplaatst naar de veilige omgeving van de [AVG Quarantaine](#). Bij de standaardinstelling zal u bij detectie van een bedreiging worden gevraagd of die naar de Quarantaine moet worden verplaatst, zodat u zeker weet dat er geen toepassingen 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 [AVG 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.*).

9.4.2. Lijst Toegestaan

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



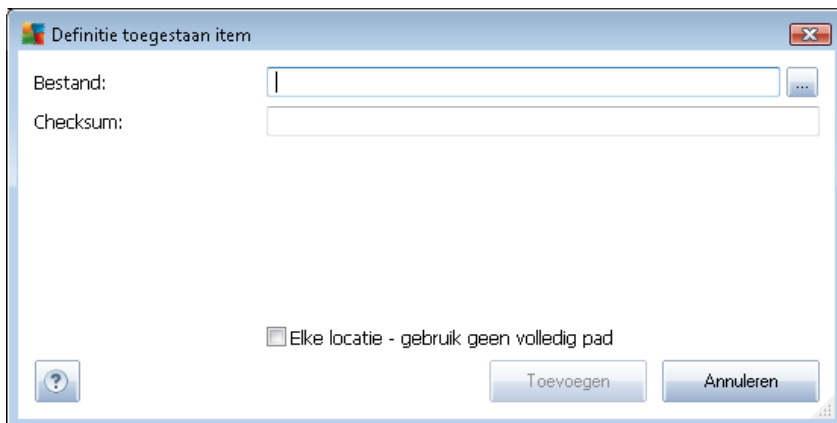
In de lijst **Identity Protection Toegestaan** staat de volgende informatie over elke toepassing:

- **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

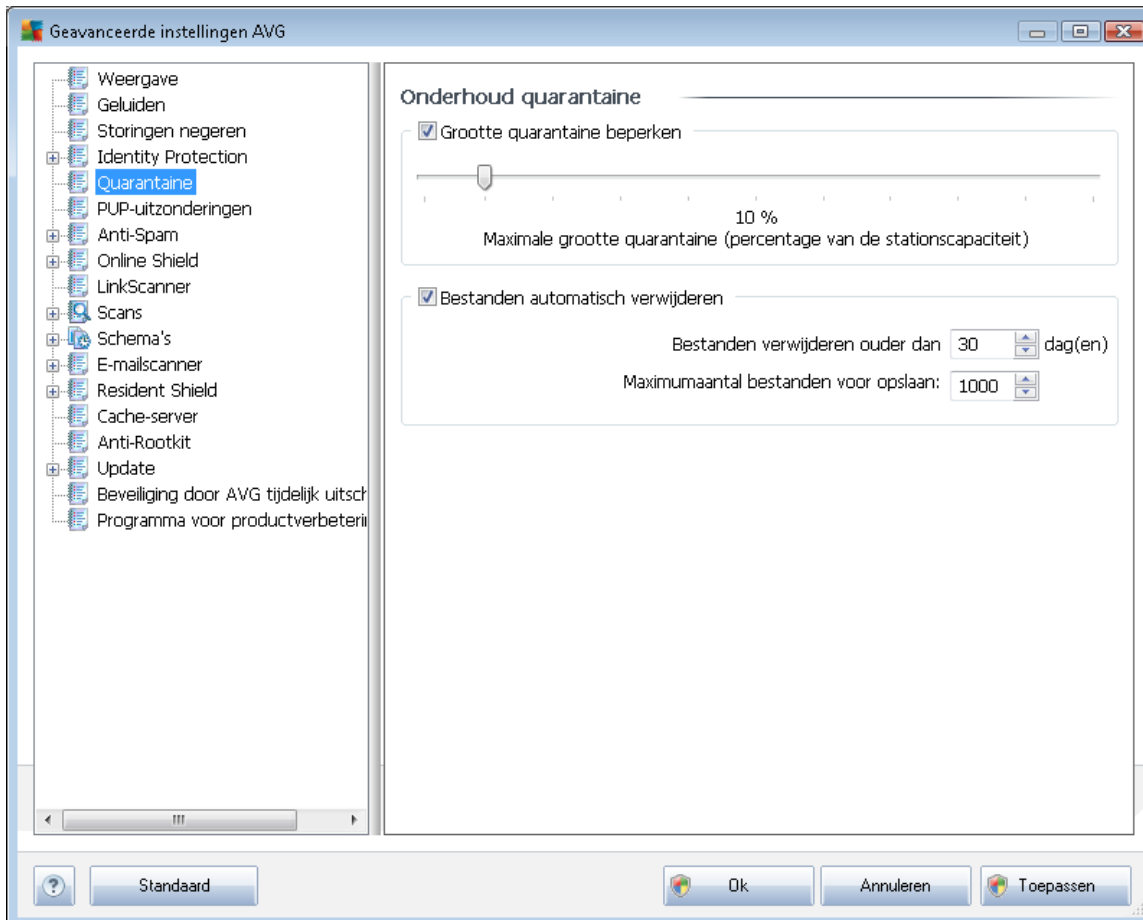
Het dialoogvenster met de **lijst Toegestaan van Identity Protection** heeft de volgende knoppen:

- **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

9.5. Quarantaine



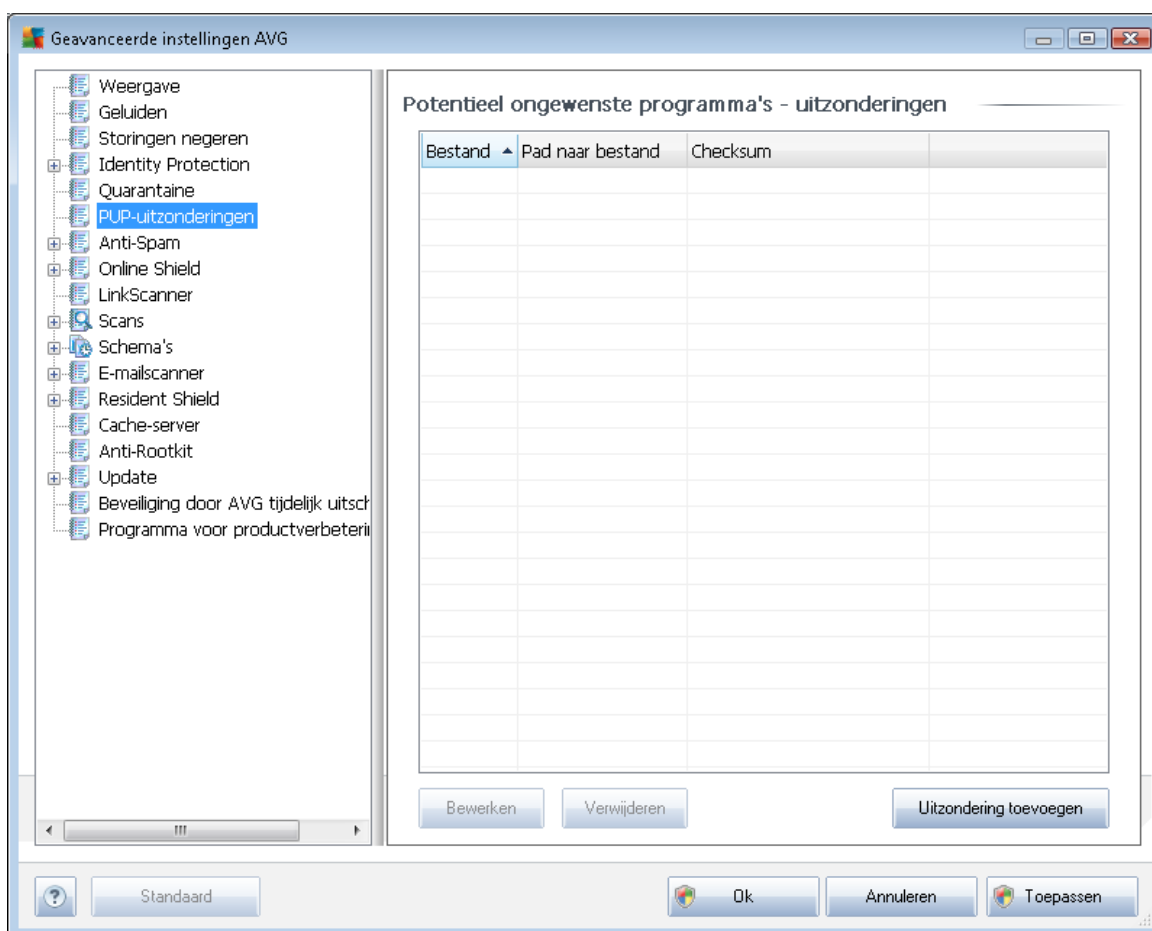
In het dialoogvenster **Onderhoud quarantaine** kunt u verschillende parameters instellen voor het beheer van objecten die zijn opgeslagen in [Quarantaine](#):

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

9.6. PUP-uitzonderingen

AVG Internet Security 2011 is in staat om uitvoerbare toepassingen en DLL-bibliotheken te analyseren en detecteren die binnen het systeem mogelijk ongewenst zijn. De gebruiker zal in sommige gevallen bepaalde gedetecteerde ongewenste programma's willen behouden (*programma's die de gebruiker opzettelijk heeft geïnstalleerd*). Sommige programma's bevatten adware. Dat is vooral het geval bij gratis programma's. Dergelijke adware wordt door AVG mogelijk gedetecteerd en

gerapporteerd als een **Potentieel ongewenst programma (PUP)**. Als u een dergelijk programma niet van uw computer wilt verwijderen, kunt u het desbetreffende programma definiëren als een uitzondering:

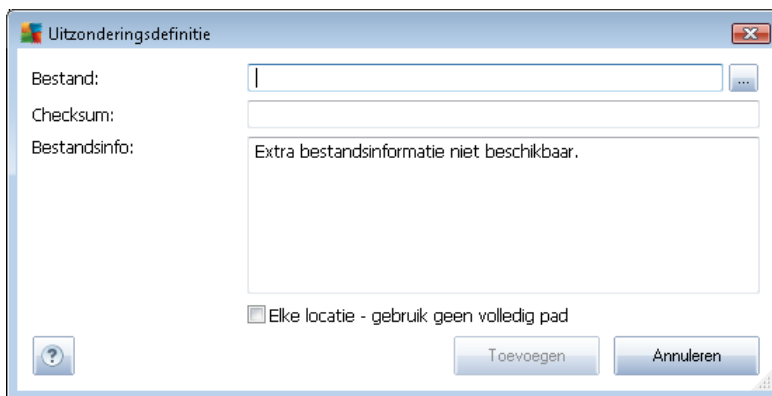


In het dialoogvenster **Uitzonderingen voor mogelijk ongewenste programma's** staat een lijst met eerder als zodanig gedefinieerde en geldige uitzonderingen op mogelijk ongewenste programma's. U kunt de lijst bewerken, bestaande items verwijderen en nieuwe uitzonderingen toevoegen. De volgende informatie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

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

Knoppen

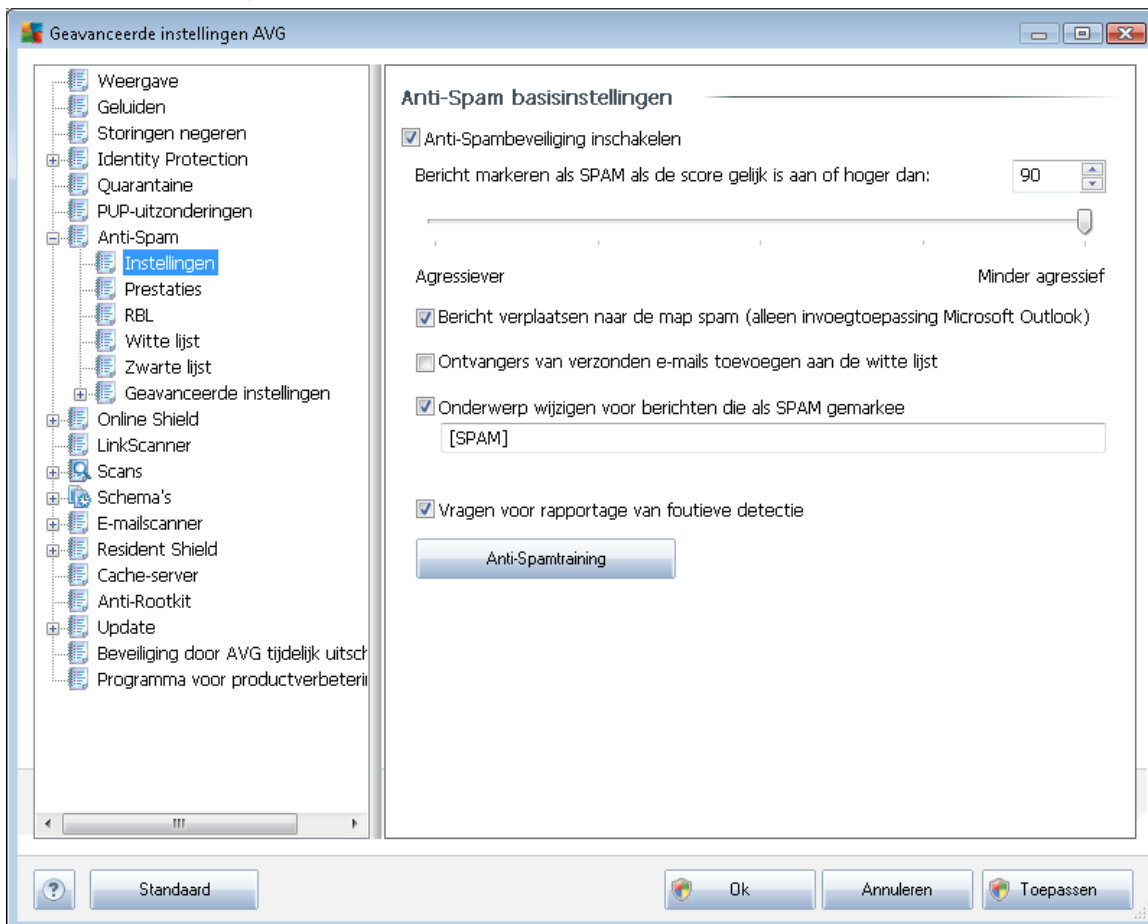
- **Bewerken** – er wordt een nieuw dialoogvenster geopend (*identiek met het dialoogvenster voor het toevoegen van een nieuwe uitzondering, zie hieronder*) voor het bewerken van een eerder gedefinieerde uitzondering, waarin u parameters kunt wijzigen
- **Verwijderen** – het geselecteerde item wordt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



- **Bestand** – Typ het volledige pad naar het bestand dat u wilt markeren als een uitzondering
- **Checksum** – de unieke "handtekening" van het gekozen bestand. Deze handtekening bestaat uit een automatisch gegenereerde tekenreeks op basis waarvan AVG het gekozen bestand onmiskenbaar van andere bestanden kan onderscheiden. Deze handtekening wordt gegenereerd en weergegeven nadat het bestand is toegevoegd.
- **Bestandsinfo** – alle aanvullende informatie die voor het bestand beschikbaar is (*licentie-/versie-informatie, enz.*)
- **Elke locatie – gebruik geen volledige locatie** – als u dit bestand alleen op deze specifieke locatie als uitzondering wilt definiëren, schakelt u dit selectievakje niet in. Als het selectievakje is ingeschakeld, is daarmee het desbetreffende bestand gekarakteriseerd als een PUP, ongeacht de locatie (*maar u dient niettemin het volledige pad naar het bestand in te voeren; het bestand wordt dan gebruikt als uniek voorbeeld voor de mogelijkheid dat twee bestanden met dezelfde naam voorkomen in uw systeem*).

9.7. Antispam

9.7.1. Instellingen



In het dialoogvenster **Basisinstellingen voor Anti-Spam** kunt u het selectievakje **Anti-Spambeveiliging inschakelen** in- en uitschakelen om het scannen van e-mail op spam in of uit te schakelen. De optie is standaard ingeschakeld en, zoals gebruikelijk, wordt aanbevolen dat alleen te veranderen als u daar een goede reden voor hebt.

In dit dialoogvenster kunt u bovendien meer of minder agressieve scoremaatregelen selecteren. Het **Anti-Spam** filter wijst een score aan elk bericht toe (*bijvoorbeeld in hoeverre de inhoud van het bericht spam benadert*) op basis van verschillende dynamische scantechnieken. U kunt de instelling **Bericht als spam markeren als score hoger is dan** aanpassen door een waarde in te voeren, of door de schuifbalk naar links of rechts te slepen (*als u de schuifbalk gebruikt, is het bereik beperkt tot 50-90*).

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

- **Waarde 80-90** – E-mailberichten waarvan de kans groot is dat ze [spam](#) bevatten, worden gefilterd. Het kan zijn dat sommige niet-spamberichten ook gefilterd worden.
- **Waarde 60-79** – Een vrij agressieve configuratie. E-mailberichten die waarschijnlijk [spam](#)



zijn, worden gefilterd. Niet-spamberichten worden waarschijnlijk ook als spam aangeduid.

- **Waarde 50-59** – Een zeer agressieve configuratie. Zowel niet-spamberichten als echte [spam](#)berichten worden gefilterd. Deze instelling is niet raadzaam voor normaal gebruik.

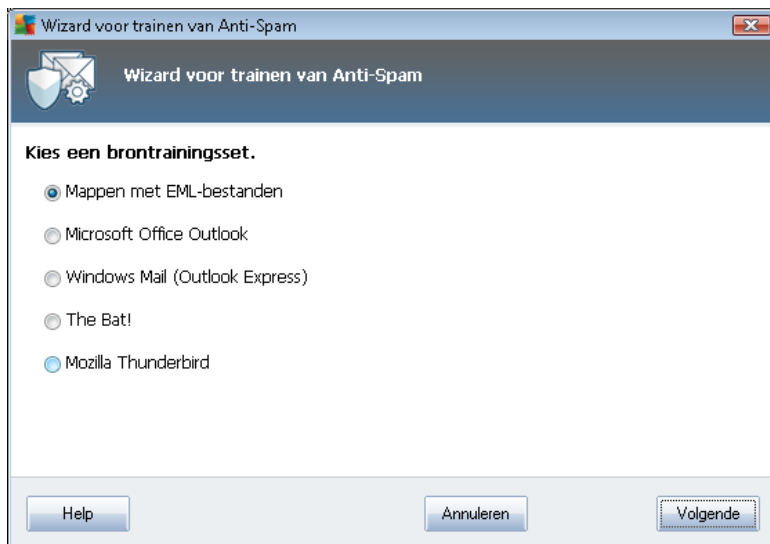
In het dialoogvenster **Basisinstellingen voor Anti-Spam** kunt u verder opgeven wat er met gedetecteerde [spam](#)berichten moet gebeuren:

- **Bericht verplaatsen naar de map spam** – schakel dit selectievakje in als elk bericht met spam dat is gedetecteerd, automatisch naar de daarvoor aangewezen map van uw e-mailclient moet worden verplaatst;
- **Ontvangers van verzonden e-mails toevoegen aan de [witte lijst](#)** – schakel dit selectievakje in om aan te geven dat alle ontvangers van verzonden e-mails kunnen worden vertrouwd, en dat e-mail die vanaf hun e-mailadressen worden verzonden, eveneens kan worden vertrouwd;
- **Onderwerp wijzigen voor berichten die als SPAM gemarkeerd zijn** – schakel dit selectievakje in als u alle berichten die als [spam](#) worden gedetecteerd, wilt markeren met een bepaald woord of teken op de onderwerpsregel van het bericht; u kunt het desbetreffende woord of teken in het geactiveerde tekstveld typen.
- **Vragen voor het rapporteren van vals alarm** – vooropgesteld dat u tijdens het [installatieproces](#) hebt aangegeven te willen deelnemen in het [productverbeteringsprogramma](#), zullen gedetecteerde bedreigingen worden gerapporteerd aan AVG. De rapportage vindt automatisch plaats. Als u echter dit selectievakje inschakelt, kunt u het rapporteren van een detectie aan AVG al dan niet bevestigen, zodat u in de gelegenheid bent vast te stellen of het bericht echt als spam moet worden geclassificeerd.

Knoppen

Anti-Spam trainen – klik op deze knop om de [wizard Anti-Spamtraining](#) te starten die gedetailleerd wordt beschreven in het [volgende hoofdstuk](#).

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



U kunt kiezen uit de volgende opties:

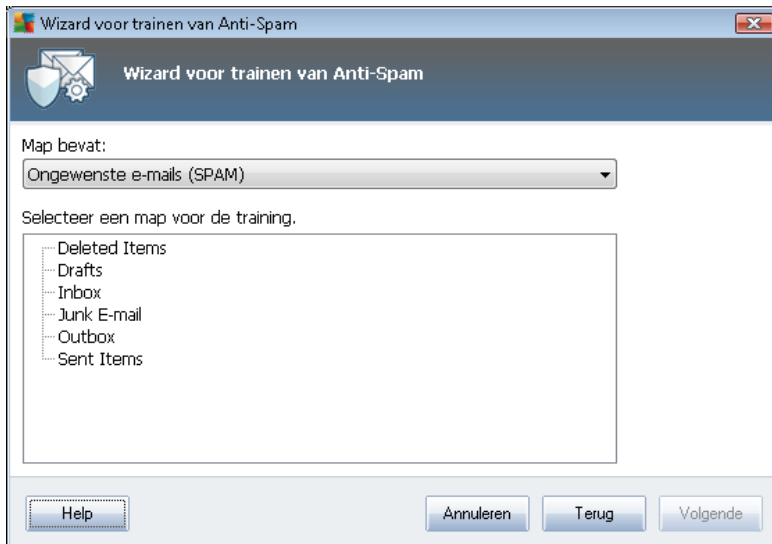
- **Een bepaalde e-mailclient** – als u met een van de genoemde e-mailclients werkt (*MS Outlook, Outlook Express, The Bat!*), selecteert u de desbetreffende optie
- **Map met EML-bestanden** - als u een ander e-mailprogramma gebruikt, dient u eerst de berichten in een bepaalde map op te slaan (*in .eml format*), of ervoor te zorgen dat u de locatie van uw map met e-mailclientberichten kent. Selecteer vervolgens **Map met EML-bestanden** om het pad naar die map op te geven

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

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

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

Mappen met EML-bestanden



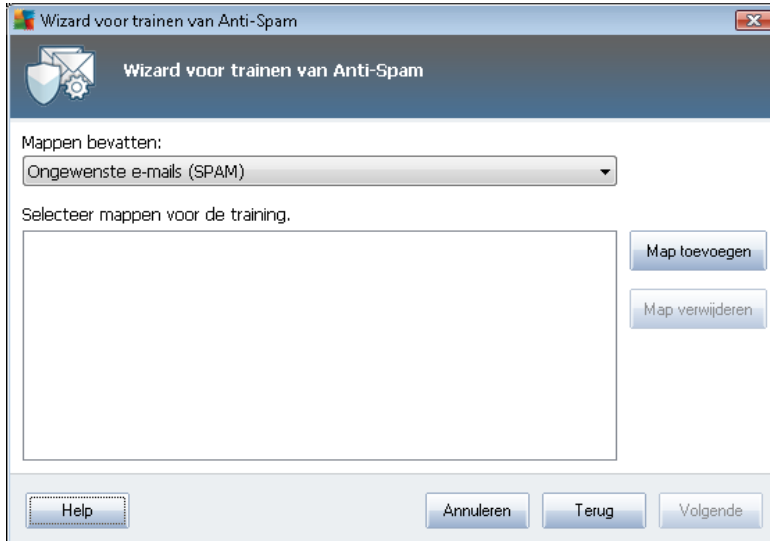
Zoek in dit dialoogvenster de map met de berichten die u wilt gebruiken voor de training. Klik op de knop **Map toevoegen** om de map te zoeken met de .eml-bestanden (*opgeslagen e-mailberichten*). De geselecteerde map zal vervolgens in het dialoogvenster worden weergegeven.

Maak met de vervolgkeuzelijst **Mappen bevatten** een keuze of de geselecteerde map gewenste berichten bevat (*HAM*) of ongewenste berichten (*SPAM*). NB: U kunt de berichten in de volgende stap filteren, dus de map hoeft niet uitsluitend trainingse-mails te bevatten. U kunt ook een ongewenste selectie van mappen in de lijst ongedaan maken door te klikken op de knop **Map verwijderen**.

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

Specifieke e-mailclient

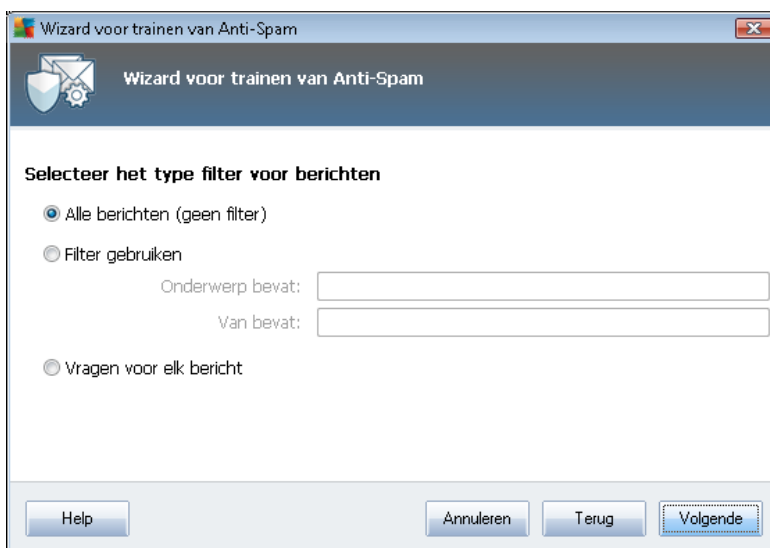
Als u een van de opties hebt bevestigd, wordt een nieuw dialoogvenster geopend.



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

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

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



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

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

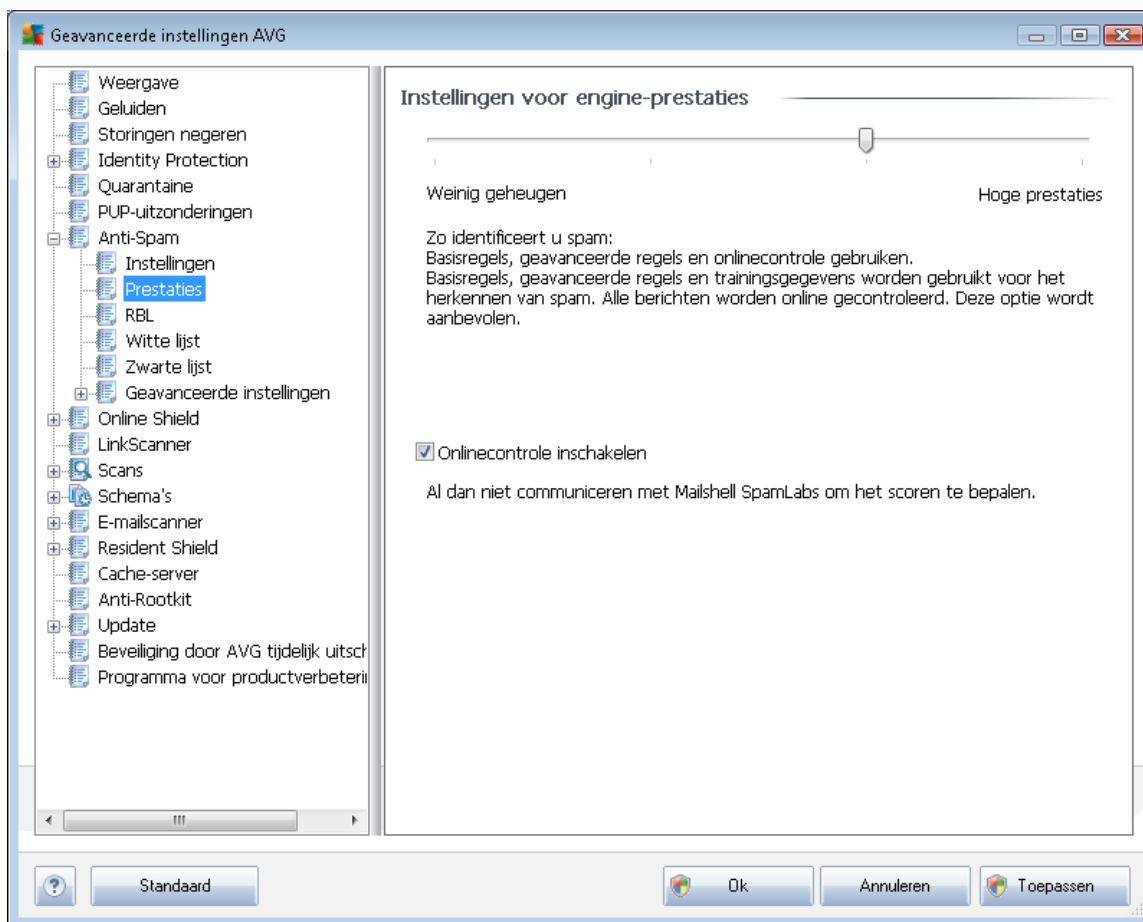
Als u niet zeker weet welke berichten in de map zitten en u wilt dat de Wizard u bij elk bericht hiernaar vraagt (zodat u kunt bepalen of u dit bericht voor training gaat gebruiken of niet), selecteert u de optie **Voor elk bericht vragen**.

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

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

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

9.7.2. Prestaties



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

Weinig geheugen / Hoge prestaties.

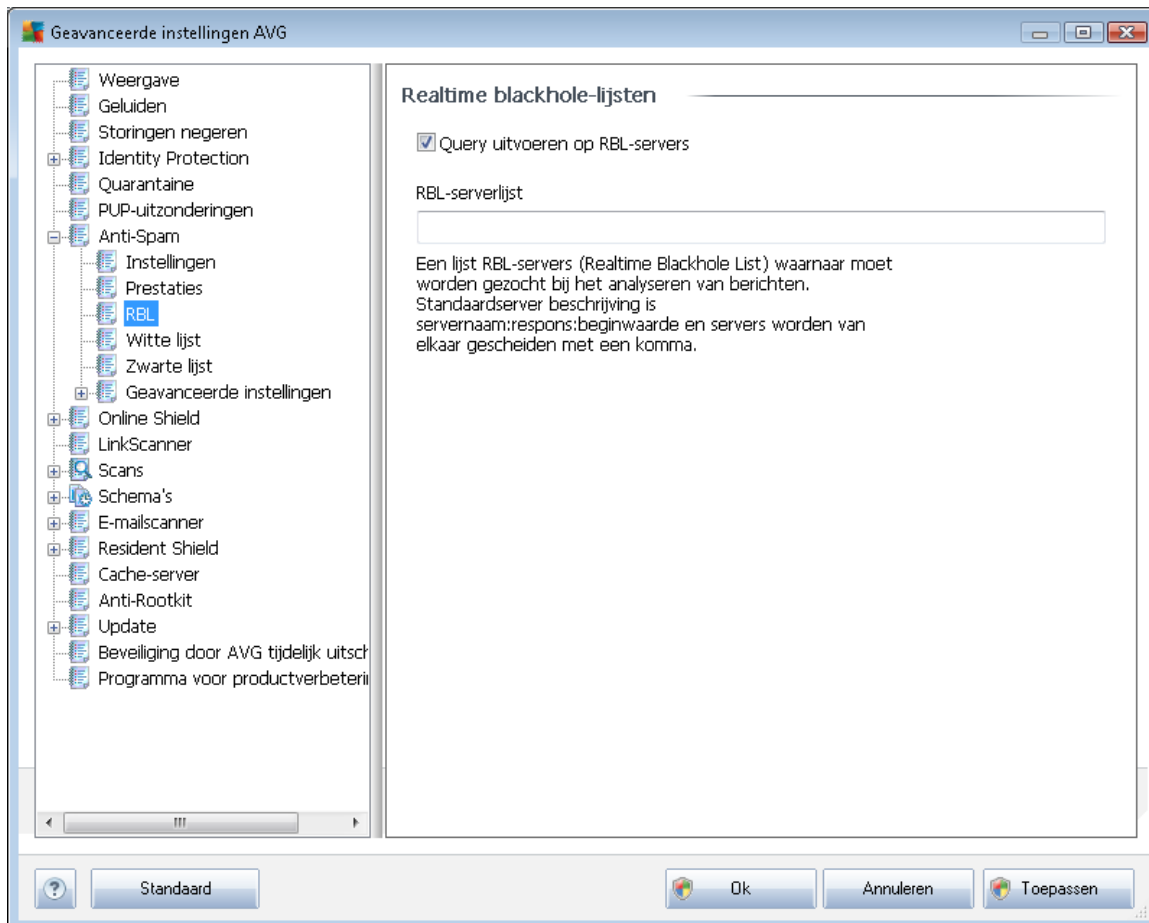
- **Weinig geheugen** – tijdens het scanproces ter detectie van [spam](#) worden geen regels gebruikt, maar alleen trainingsgegevens. Het is niet raadzaam deze modus voor normaal gebruik te selecteren, tenzij de computerhardware van lage kwaliteit is.
- **Hoge prestaties** – bij deze stand wordt een groot beroep gedaan op het geheugen van de computer. Bij het scanproces ter detectie van [spam](#) worden de volgende functies gebruikt: regels en [spam](#)database, basisregels, geavanceerde regels, IP-adressen van spammers en spammerdatabases.

De optie **Online controle inschakelen** is standaard ingeschakeld. Dit resulteert in een meer precieze [spam](#)detectie dankzij communicatie met de [Mailshell](#) servers, dat wil zeggen dat de gescande gegevens online worden vergeleken met [Mailshell](#) databases.

Over het algemeen is het raadzaam de standaardinstellingen aan te houden en die alleen te wijzigen als u daar een goede reden voor hebt. Wijzigen van deze configuratie is voorbehouden aan experts!

9.7.3. RBL

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





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

De RBL-server (*Realtime Blackhole List*) is een DNS-server met een uitgebreide database van bekende spammers. Wanneer deze functie ingeschakeld is, worden alle e-mailberichten gecontroleerd in de RBL-serverdatabase en als [spam](#) gemarkeerd wanneer ze identiek zijn aan een onderdeel van de database. De RBL-serverdatabases bevatten de recentste spamvingerafdrukken, waardoor de beste en meest accurate [spam](#)detectie geboden kan worden. Deze functie is vooral nuttig voor gebruikers die grote hoeveelheden spam ontvangen die normaal niet door de [Anti-Spam](#)-engine gedetecteerd wordt.

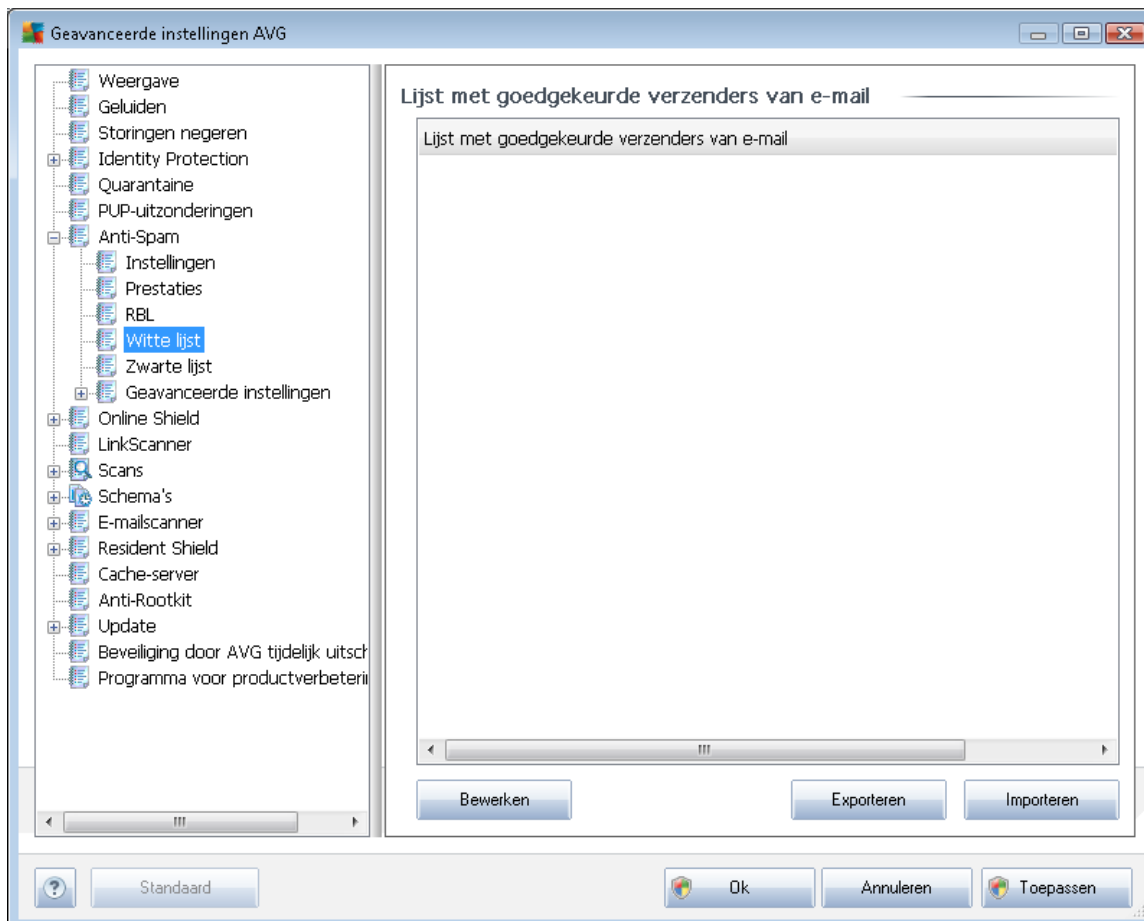
Op de **RBL-serverlijst** kunt u specifieke RBL-serverlocaties definiëren.

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

Er worden geen persoonlijke gegevens naar de server verzonden!

9.7.4. Witte lijst

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



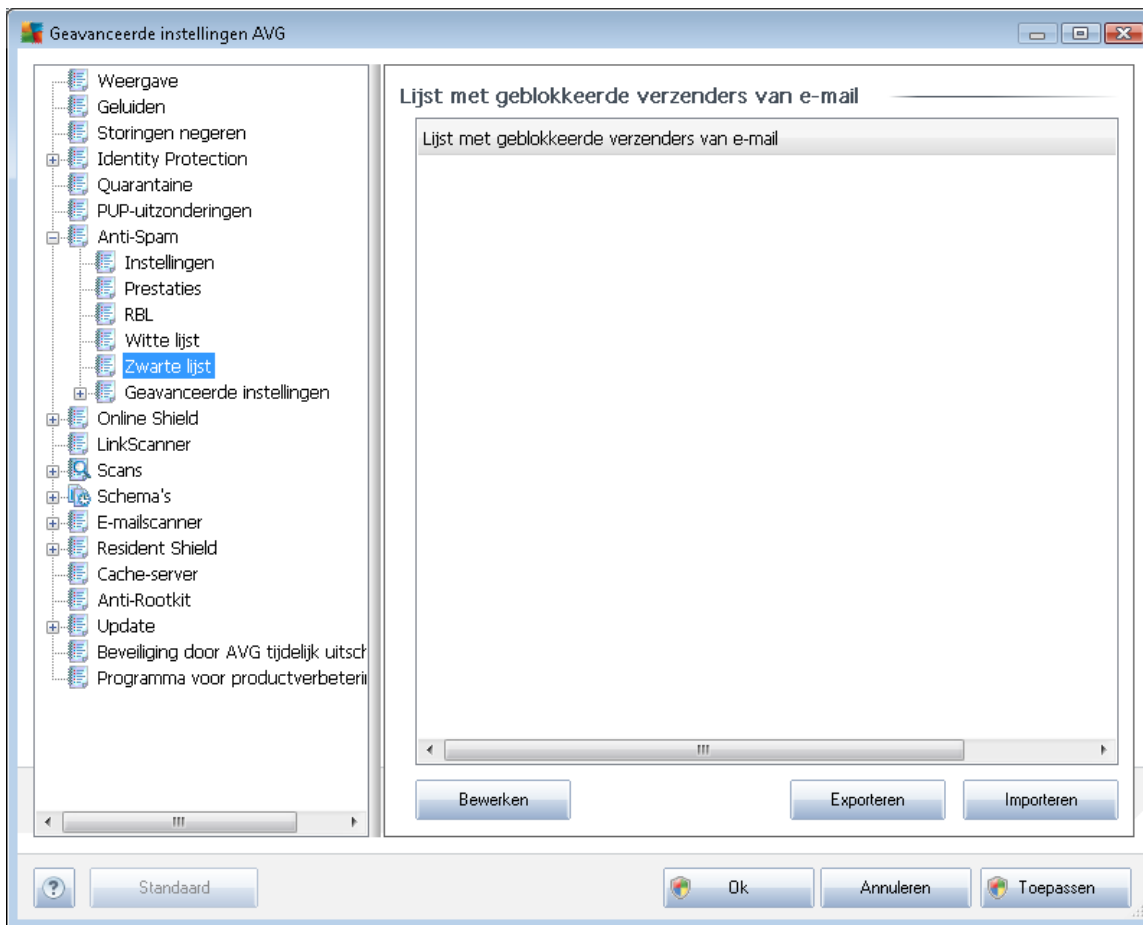
U kunt in het tekstverwerkingsgedeelte een lijst samenstellen met afzenders waarvan u zeker weet dat ze u geen ongewenste e-mail ([spam](#)) zullen sturen. U kunt ook een lijst samenstellen met domeinnamen (*bijvoorbeeld avg.com*), waarvan u weet dat ze geen spam genereren.

Als u eenmaal zo'n lijst met afzenders/domeinnamen hebt samengesteld, kunt u die op twee manieren invoeren: rechtstreeks elk e-mailadres afzonderlijk of in één keer door het importeren van de lijst. De volgende knoppen zijn beschikbaar:

- **Bewerken** – klik op deze knop om een dialoogvenster te openen waarin u handmatig een lijst met adressen kunt invoeren (*u kunt ook kopiëren en plakken*). Voeg één item (*afzender, domeinnaam*) per regel in.
- **Exporteren** - als u de gegevens wilt exporteren, klikt u op deze knop. Alle gegevens worden dan naar een tekstbestand opgeslagen.
- **Importeren** – Als u al een tekstbestand met e-mailadressen/domeinnamen hebt gemaakt, kunt u die gewoon importeren door op deze knop te klikken. In het bestand mag op iedere regel slechts één item (*adres, domeinnaam*) staan.

9.7.5. Zwarte lijst

Met de optie **Zwarte lijst** opent u een dialoogvenster met een globale lijst met geblokkeerde e-mailadressen en domeinnamen. De berichten van deze afzenders worden altijd als [spam](#) gemarkeerd.



U kunt in het tekstverwerkingsgedeelte een lijst samenstellen met afzenders waarvan u ongewenste e-mail verwacht ([spam](#)). U kunt ook een lijst met volledige domeinnamen samenstellen (zoals *spammingbedrijf.nl*), waarvan u spamberichten verwacht of ontvangt. Alle e-mailberichten die worden ontvangen van de weergegeven adressen/domeinen, worden gemarkeerd als spam.

Als u eenmaal zo'n lijst met afzenders/domeinnamen hebt samengesteld, kunt u die op twee manieren invoeren: rechtstreeks elk e-mailadres afzonderlijk of in één keer door het importeren van de lijst. De volgende knoppen zijn beschikbaar:

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



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

9.7.6. Geavanceerde instellingen

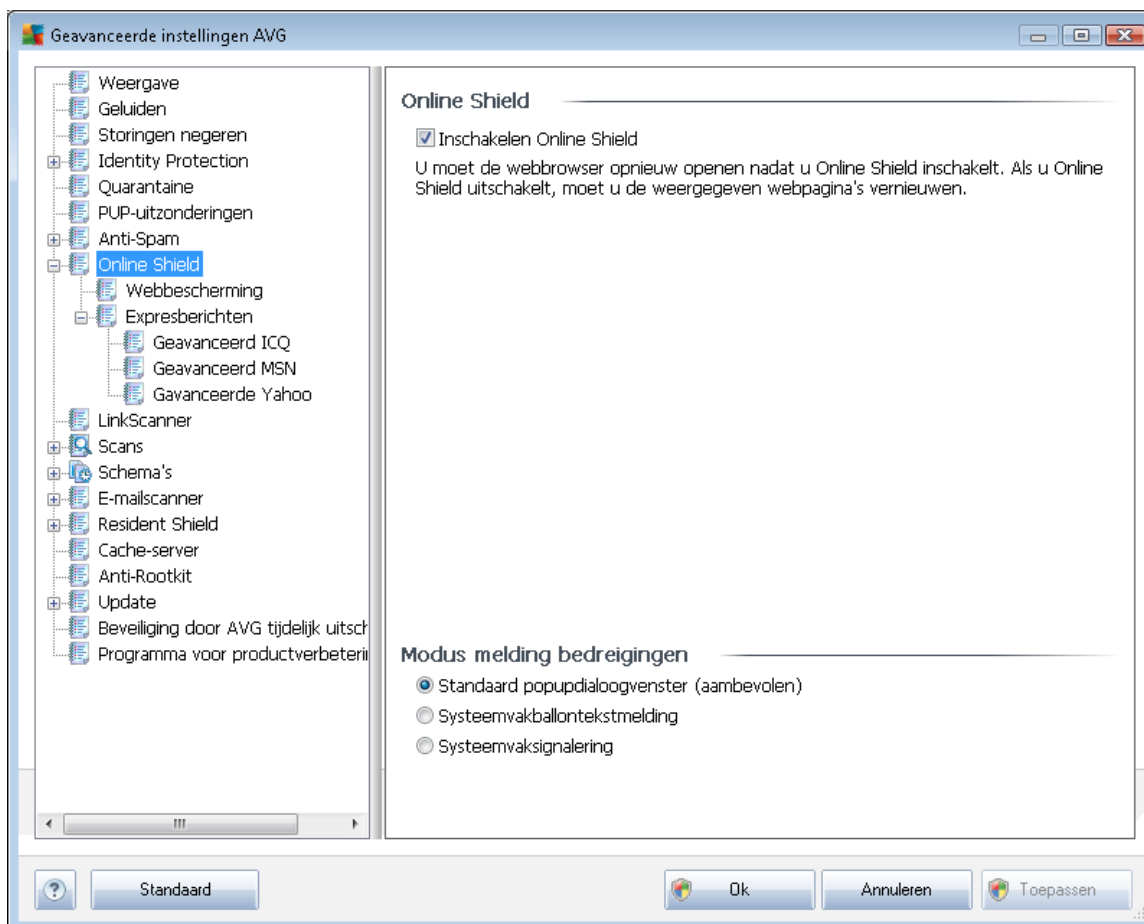
Het onderdeel Geavanceerde instellingen bevat uitgebreide instelopties voor het onderdeel Anti-Spam. Die instellingen zijn bedoeld voor ervaren gebruikers, met name voor netwerkbeheerders die de beveiliging tegen spam tot in detail moeten configureren om e-mailservers optimaal te kunnen beschermen. Om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

We raden u echter nadrukkelijk aan om geen instellingen te wijzigen, tenzij u volledig vertrouwd bent met de geavanceerde instellingen van Spamcatcher (MailShell Inc.). Onjuiste wijzigingen in het bestand kunnen leiden tot slechte prestaties of een onjuiste functionaliteit van het onderdeel.

Als u nog steeds van mening bent dat u de configuratie van [Anti-Spam](#) op het geavanceerde niveau wilt wijzigen, volgt u de instructies die in de gebruikersinterface worden weergegeven. Over het algemeen is elk dialoogvenster gewijd aan één specifieke functie die u dan kunt wijzigen – de beschrijving van de functie staat steeds in datzelfde dialoogvenster:

- **Cache** – Vingerafdruk, Domeinreputatie, LegitRepute
- **Training** – max in te voeren woorden, drempel autotraining, gewicht
- **Filteren** – Taallijst, Landenlijst, Goedgekeurde IP's, Geblokkeerde IP's, Geblokkeerde landen, Geblokkeerde tekensets, Spoof-verzenders
- **RBL** – RBL-servers, Multihit, Drempel, Time-out, Max IP's
- **Internetverbinding** – Time-out, Proxyserver, Proxyserververificatie

9.8. Online Shield



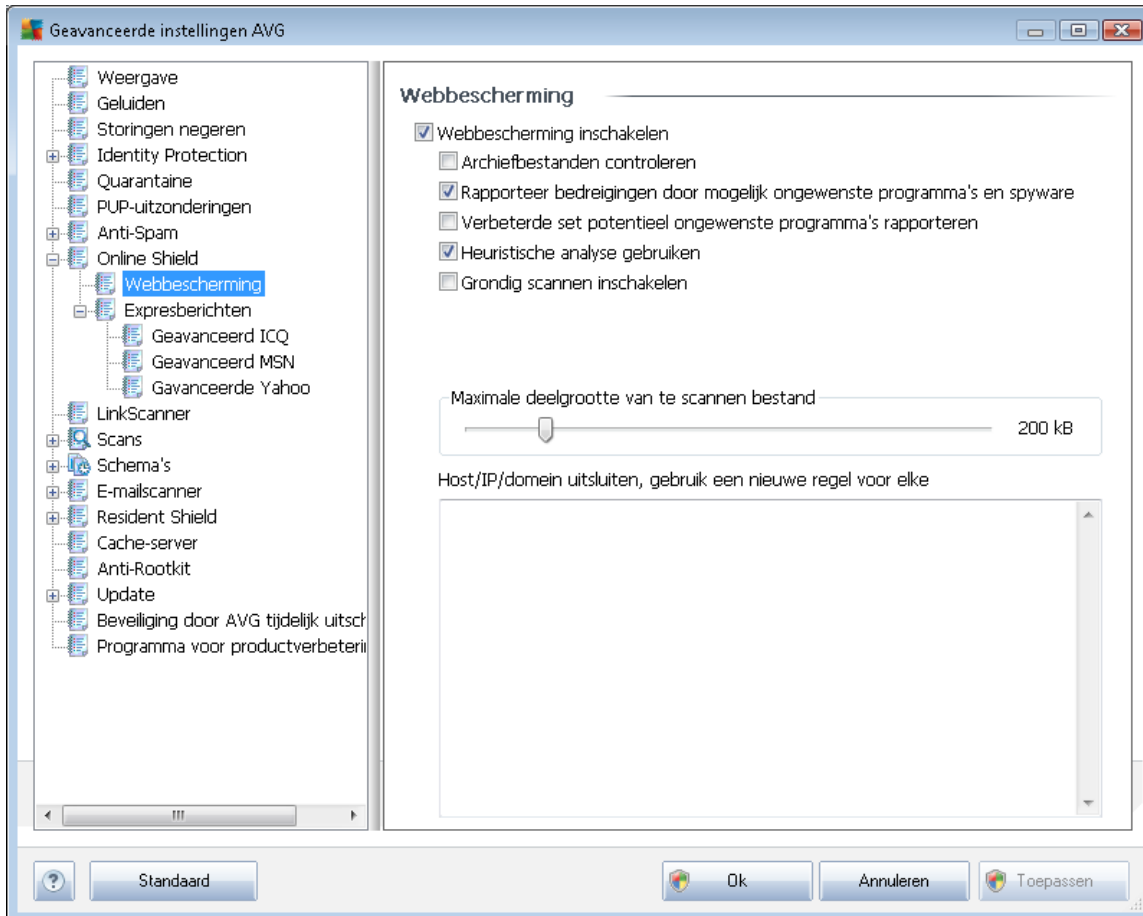
In het dialoogvenster **Online Shield** kunt u het volledige onderdeel **Online Shield** in- en uitschakelen via de optie **Online Shield inschakelen** (standaard ingeschakeld). Voor verdere geavanceerde instellingen voor dit onderdeel verwijzen we u naar de desbetreffende dialoogvensters die in de navigatiestructuur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

- [Webbescherming](#)
- [Expresberichten](#)

Modus melding bedreigingen

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

9.8.1. Webbescherming



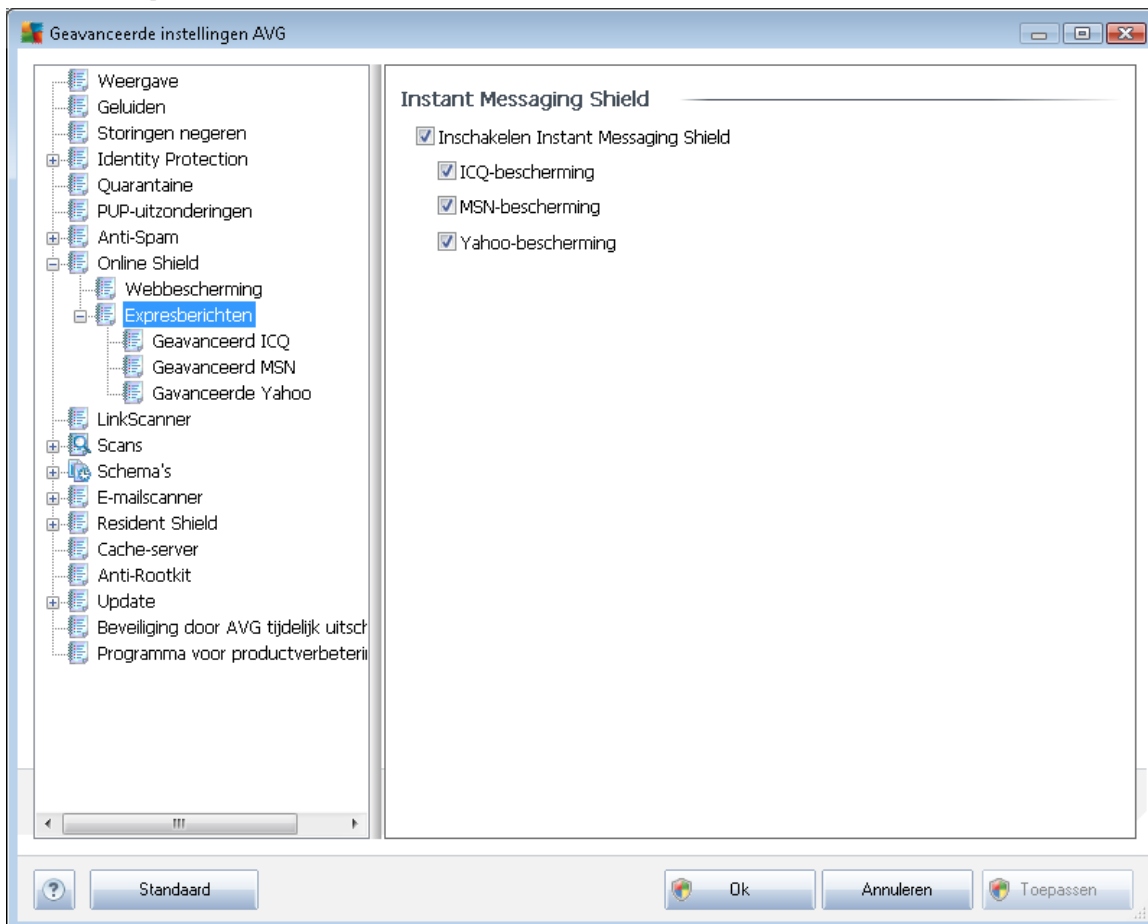
In het dialoogvenster **Webbescherming** kunt u de configuratie van het onderdeel aanpassen met betrekking tot het scannen van de inhoud van websites. U kunt de volgende basisopties aanpassen:

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

9.8.2. Expresberichten

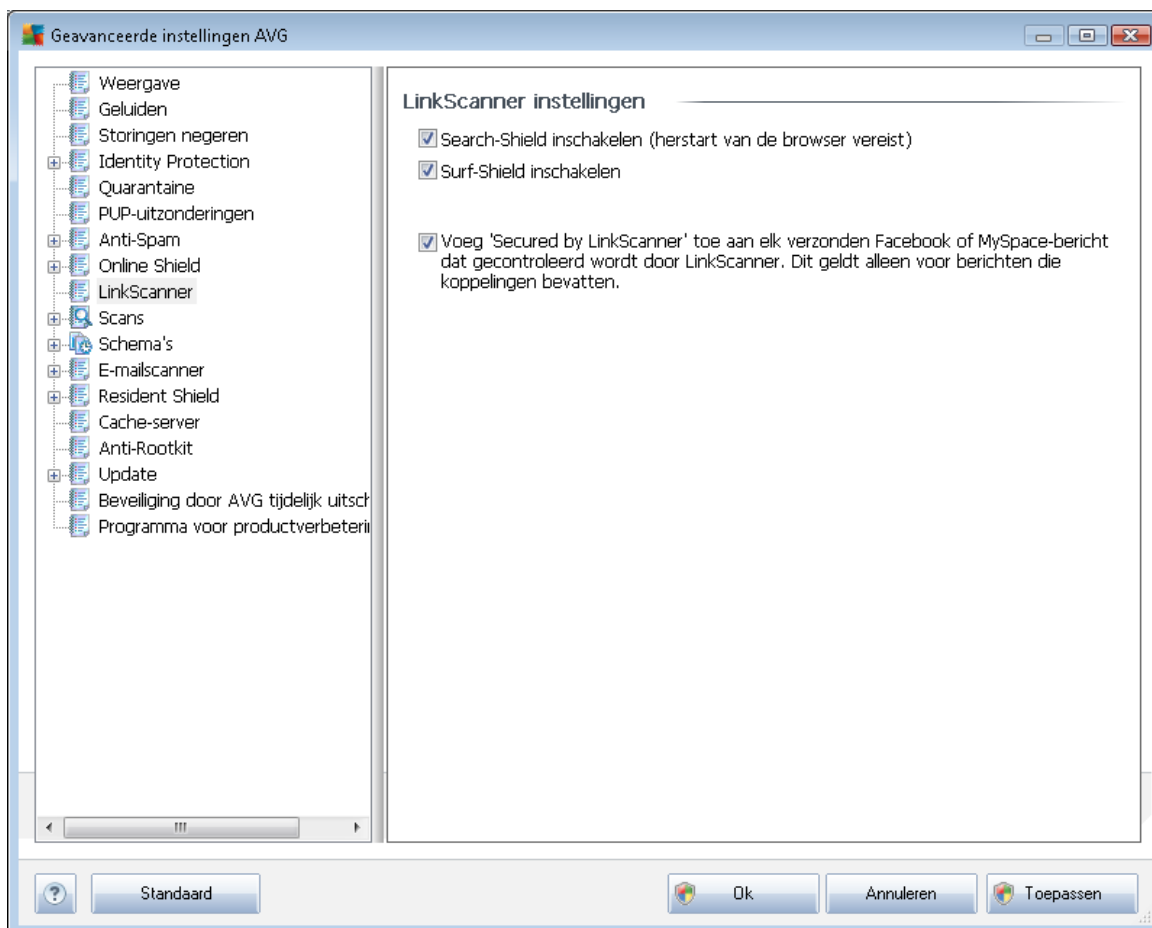


In het dialoogvenster **Instant Messaging Shield** kunt u de instellingen van het onderdeel **Online Shield** bewerken die betrekking hebben op het scannen van expresberichten. Op dit moment worden de volgende drie programma's voor expresberichten ondersteund: **ICQ**, **MSN** en **Yahoo** - schakel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

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

9.9. 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' ... - ' ...** – een certificatiemelding over een **LinkScanner**-scan toevoegen aan alle berichten met actieve hyperlinks, verzonden via de sociale netwerken Facebook en MySpace.



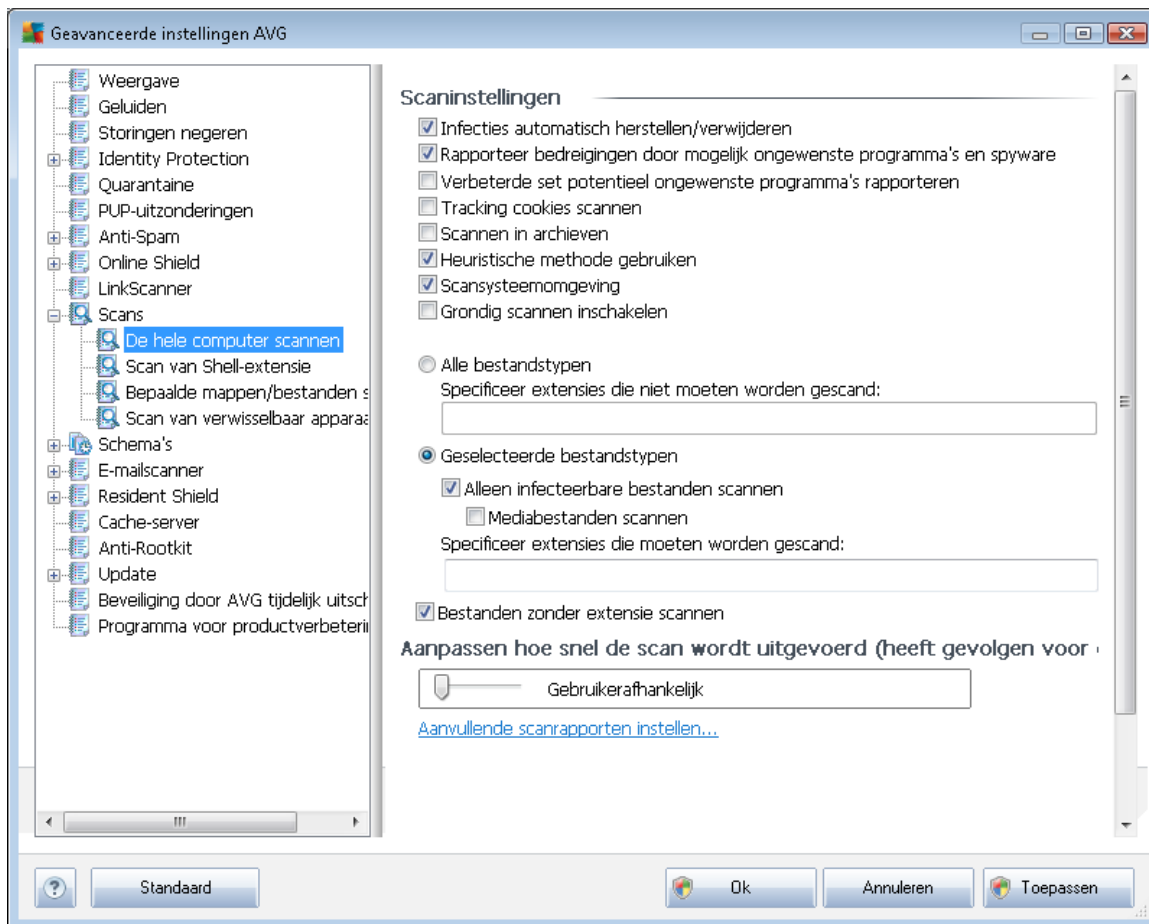
9.10. Scans

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](#) – 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

9.10.1. De hele computer scannen

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



Scaninstellingen

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

- **Infecties automatisch herstellen/verwijderen** (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 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.

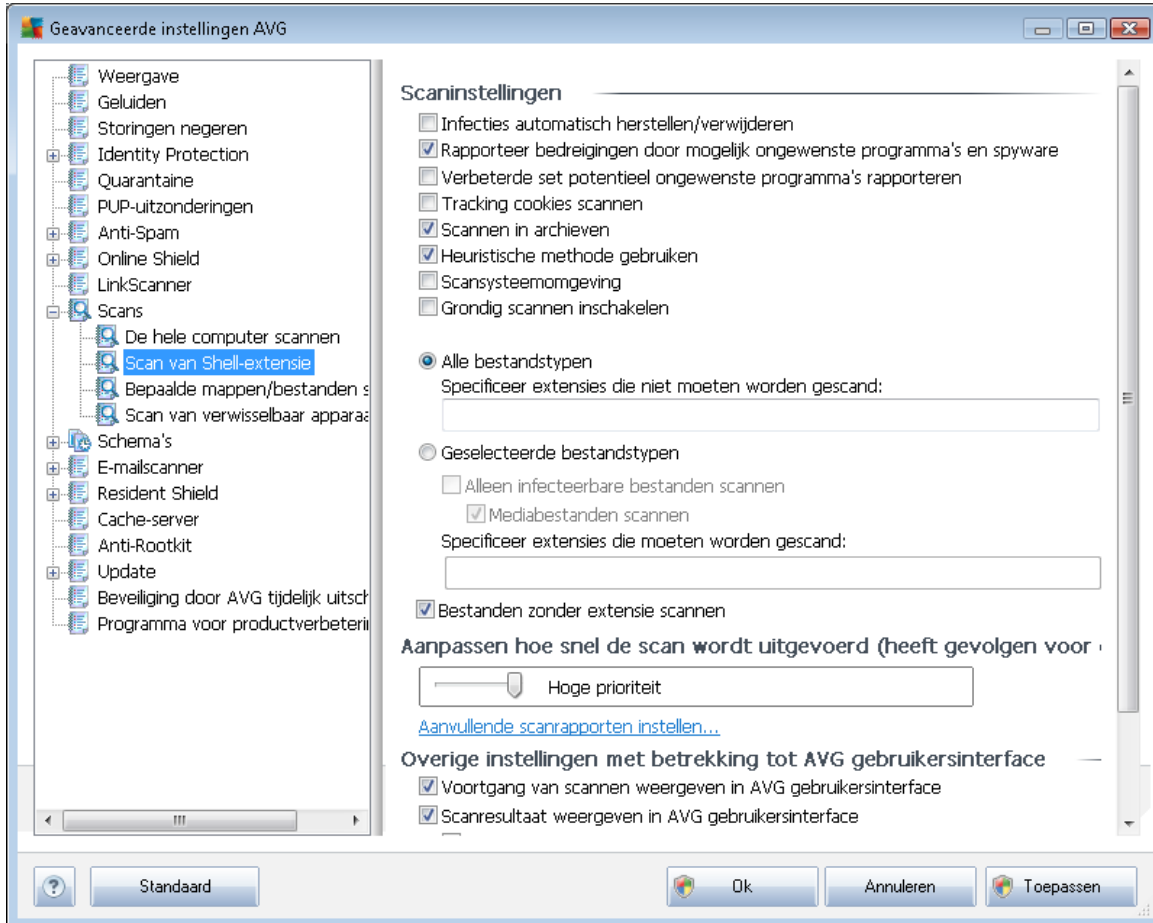
Aanvullende scanrapporten instellen...

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:



9.10.2. Shell-extensiescan

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



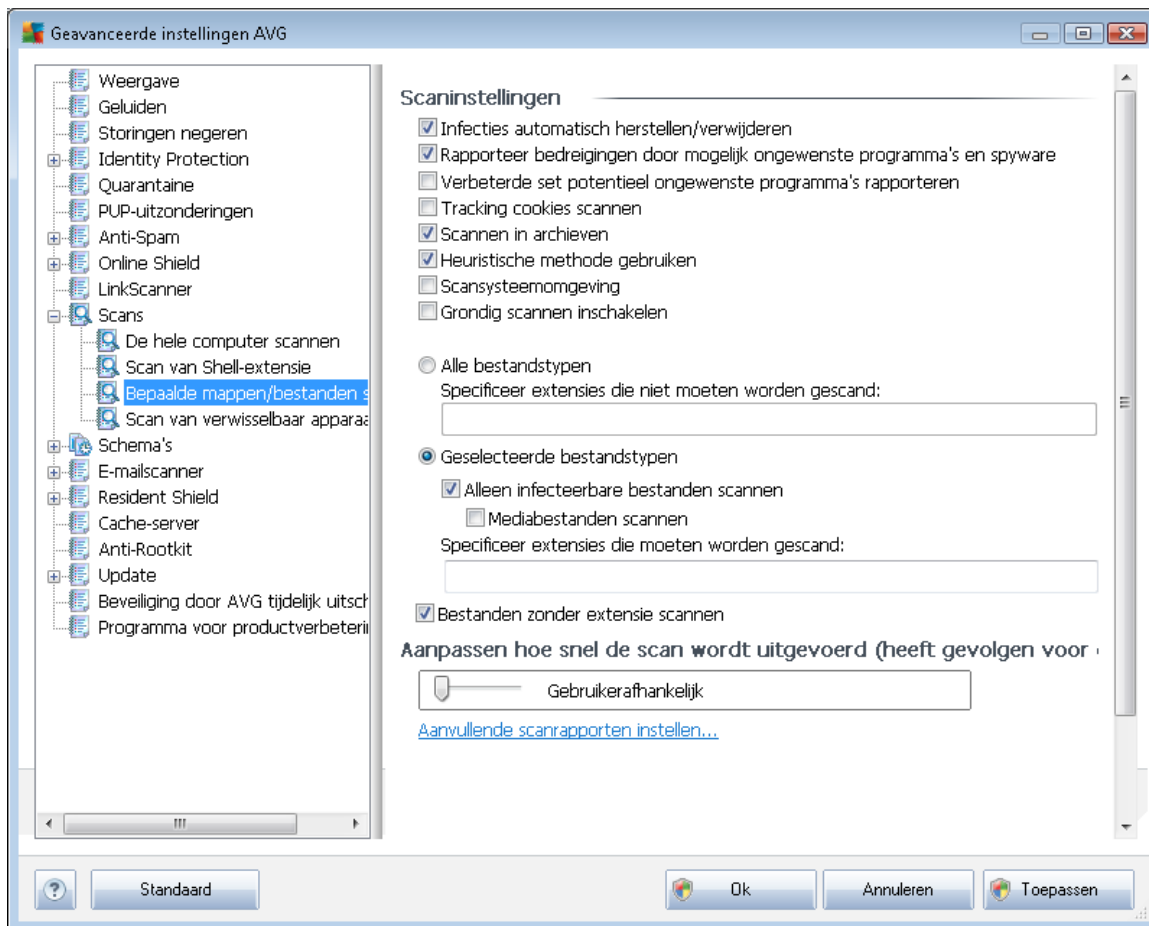
De lijst met beschikbare parameters is dezelfde als die van [De hele computer scannen](#). De standaardinstellingen verschillen echter (*bij het scannen van de hele computer worden bijvoorbeeld archiefbestanden overgeslagen, maar wordt de systeemomgeving wel gescand, terwijl het bij de Shell-extensiescan 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 **Shell-extensiescan** 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 vanuit de gebruikersinterface van AVG bereikbaar moeten zijn. Bovendien kunt u opgeven dat het scanresultaat alleen moet worden weergegeven als er tijdens het scannen een infectie is gedetecteerd.

9.10.3. Bepaalde mappen of bestanden scannen

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

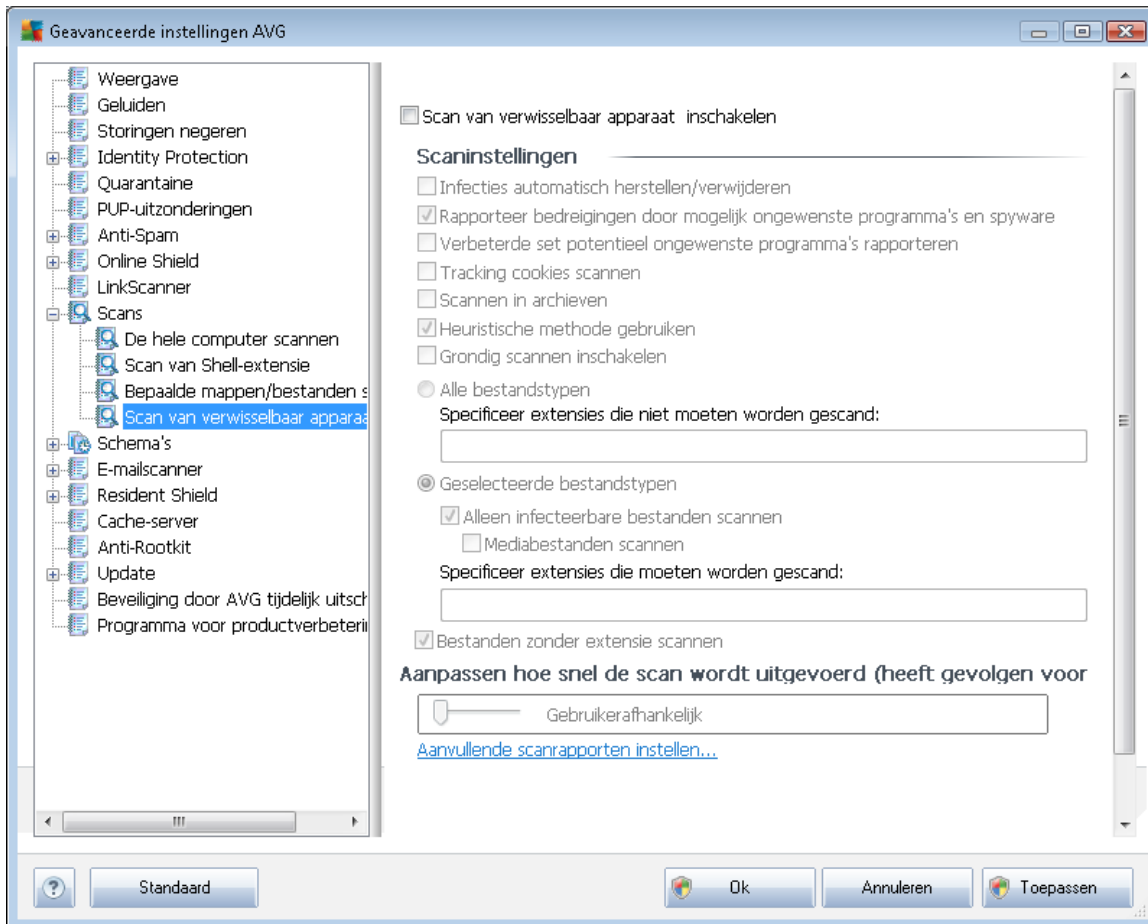


Alle parameters die u instelt in dit configuratiedialogvenster hebben alleen betrekking op het scannen met de optie **Bepaalde mappen of bestanden scannen!**

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

9.10.4. Scan van verwisselbaar apparaat

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



De **Scan van verwisselbaar apparaat** wordt automatisch uitgevoerd wanneer u een verwisselbaar 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.

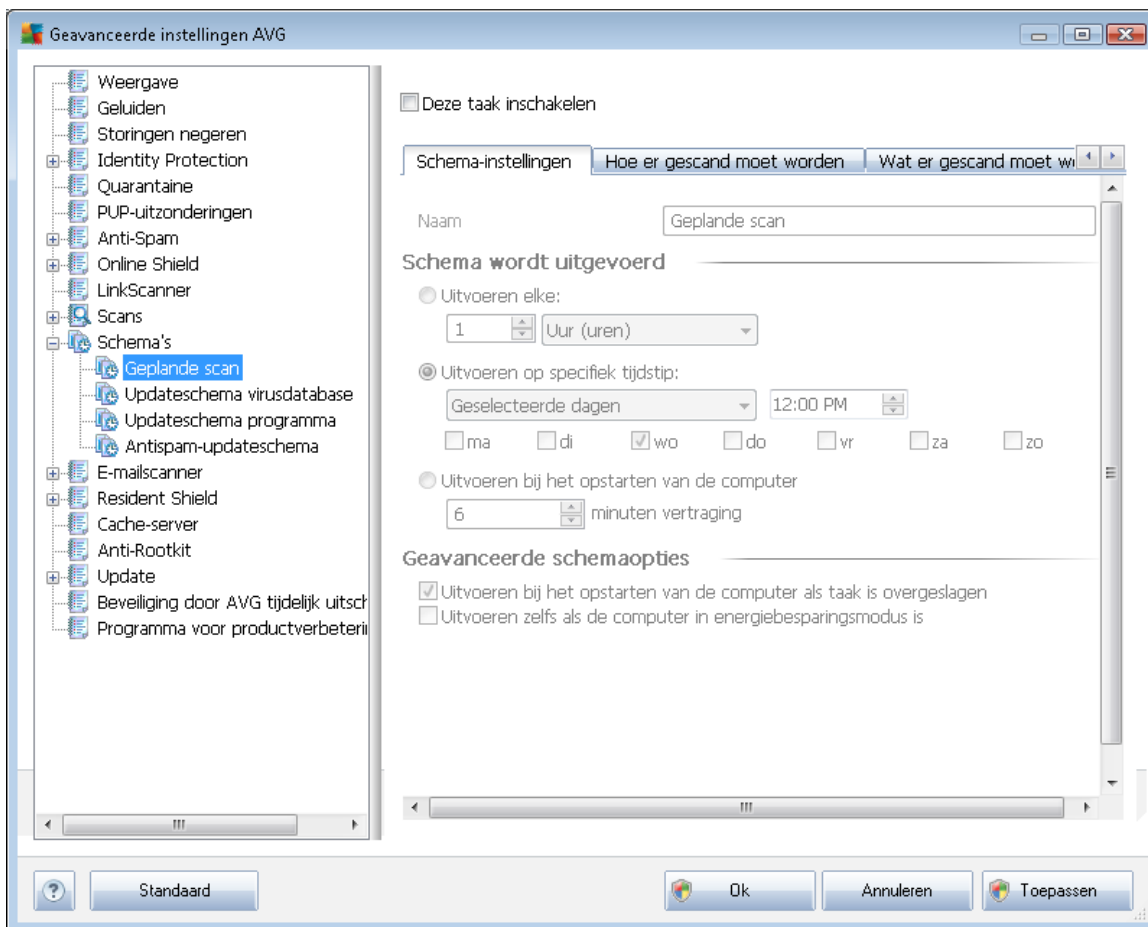
9.11. Schema's

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

- [Geplande scan](#)
- [Updateschema virusdatabase](#)
- [Updateschema programma](#)
- [Updateschema Anti-Spam](#)

9.11.1. 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 aanwijding geven van wat de scan doet. Een naam als "Scan systeemgebieden" is daarentegen een voorbeeld van een veelzeggende naam voor een scan. Bovendien is het niet nodig om in de naam van de scan aan te geven of de hele computer wordt gescand of alleen een selectie van mappen en bestanden – uw eigen scans zijn altijd aangepaste versies van het type [Bepaalde mappen of bestanden scannen](#).



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

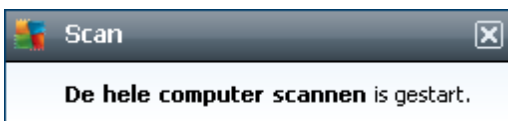
Schema wordt uitgevoerd

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

Geavanceerde schemaopties

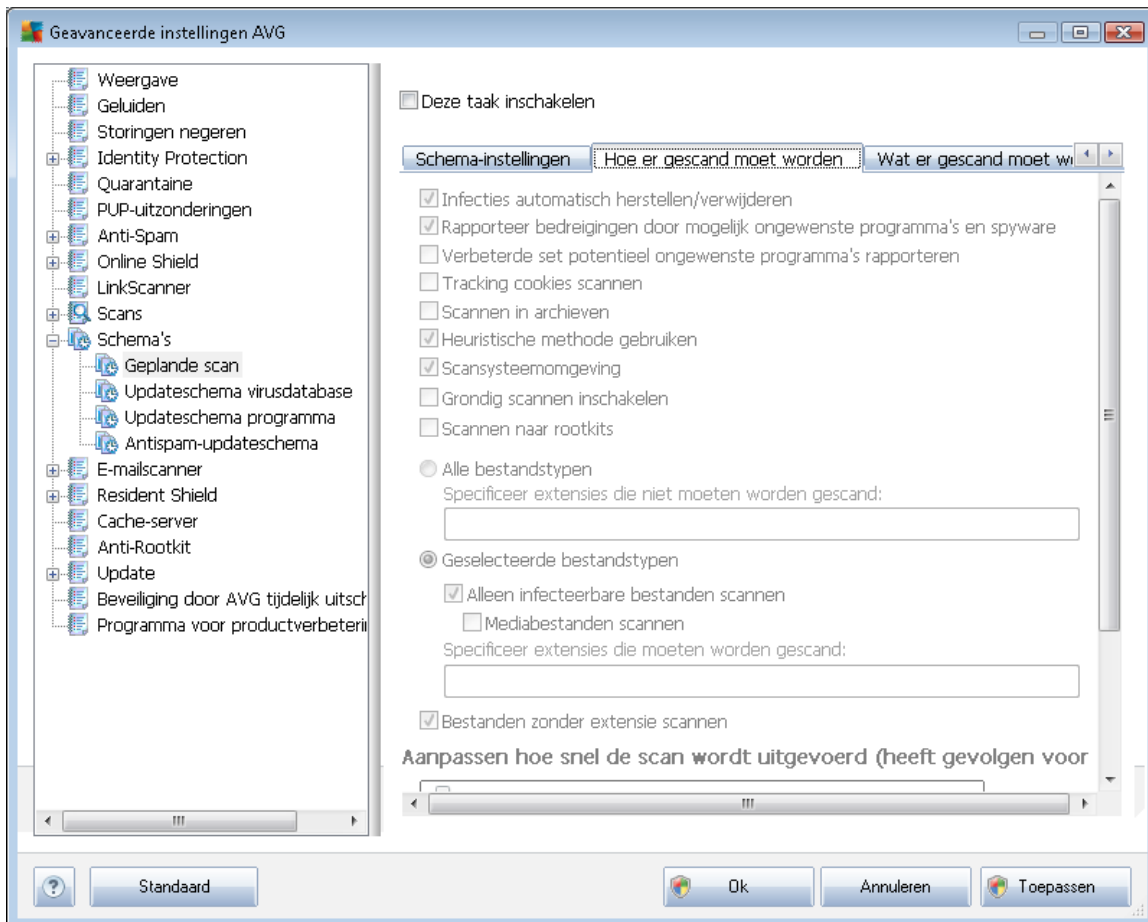
In deze sectie kunt u bepalen onder welke omstandigheden de scan wel of niet moet worden uitgevoerd als de computer in een energiebesparingsmodus is of helemaal is uitgeschakeld.

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



Vervolgens verschijnt er een nieuw [systeemvakpictogram van AVG](#) (in kleur met een 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 *gebruik erafhankelijk* 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 gebruik maakt*). U kunt echter het beroep op systeembronnen ook verkleinen door te kiezen voor een langere scanduur.

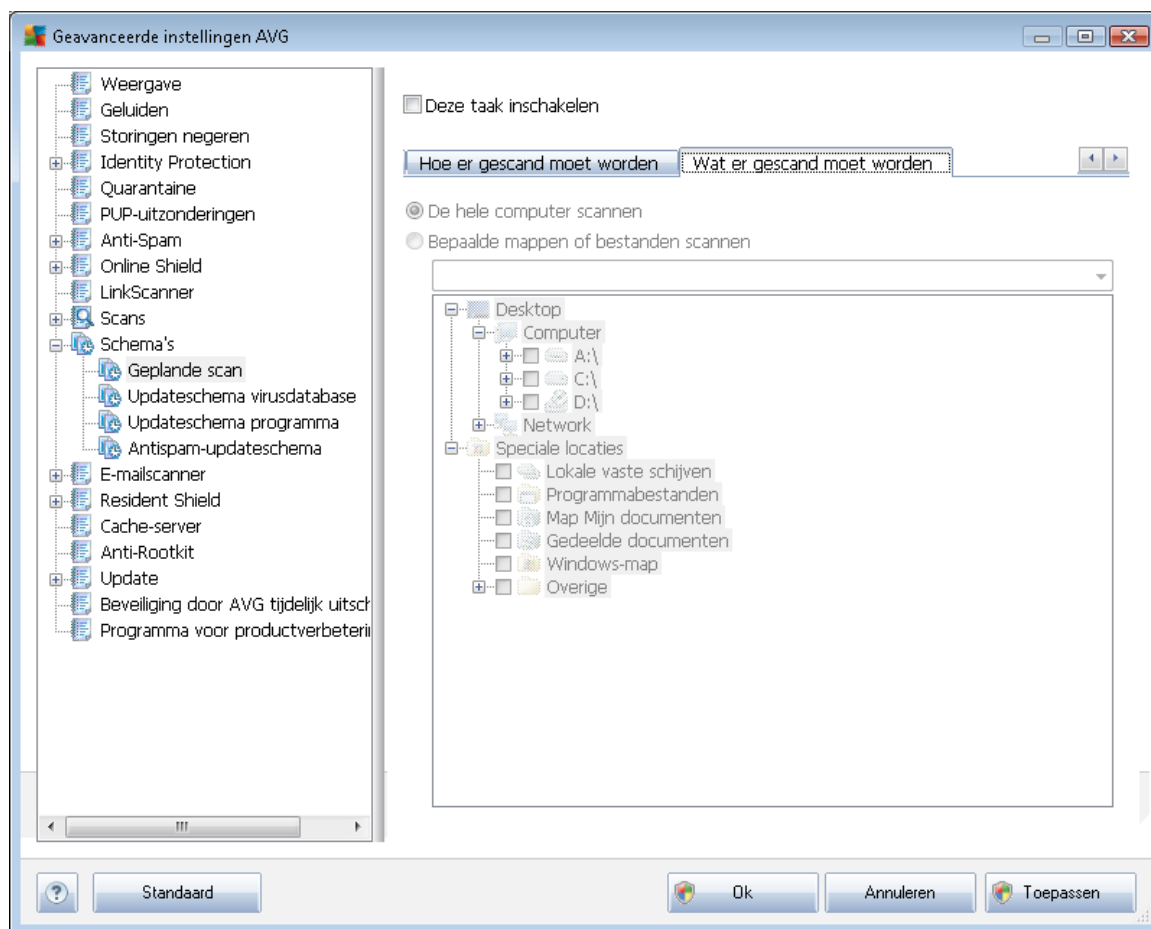
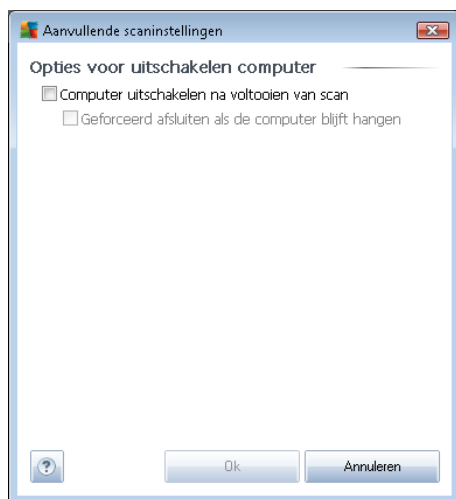
Aanvullende scanrapporten instellen

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 computerte** 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 voltooiën 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**).

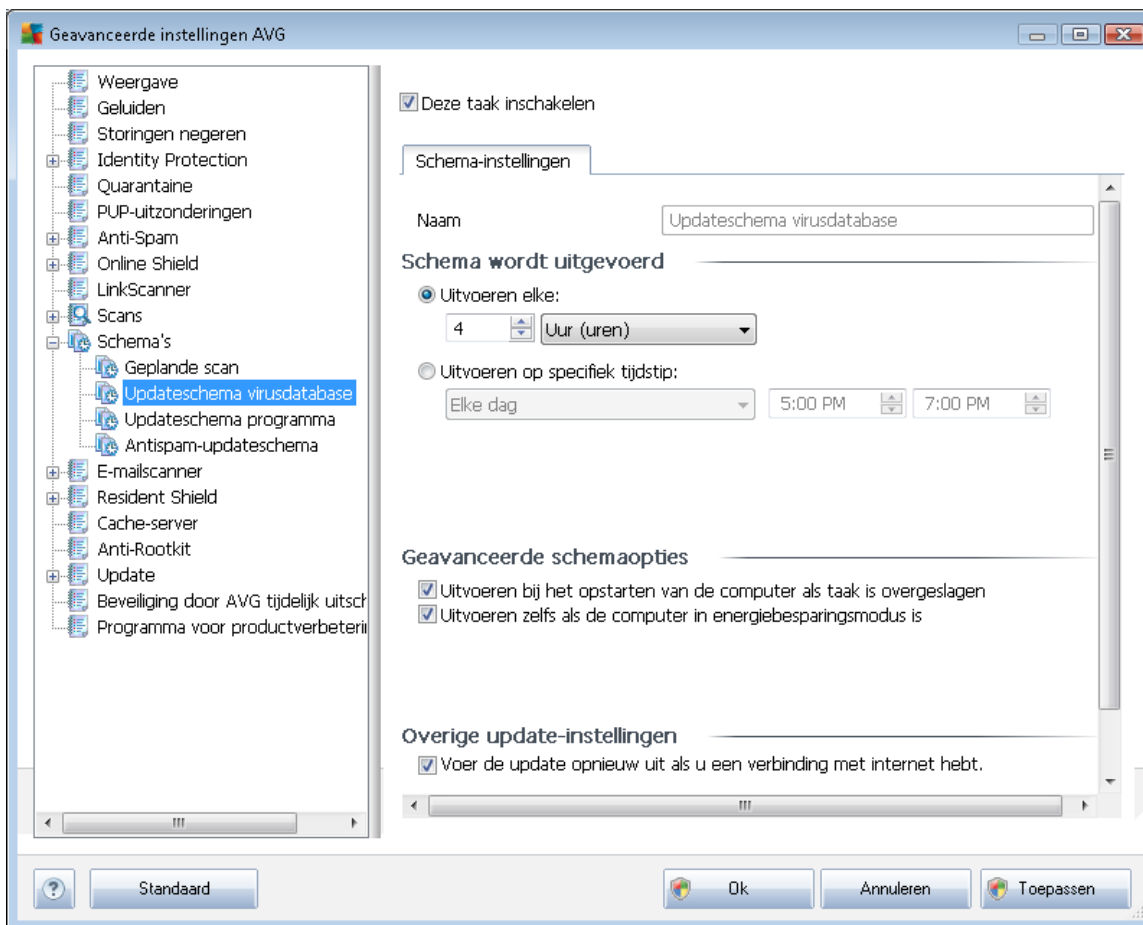


Op het tabblad ***Wat er gescand moet worden*** kunt u opgeven welke scan moet worden uitgevoerd: [een scan van de hele computer](#) of [een scan van specifieke bestanden of mappen](#). Als u kiest voor het scannen van specifieke bestanden of mappen, wordt de in het onderste deel van het

dialogvenster weergegeven mapstructuur actief, zodat u mappen kunt opgeven die moeten worden gescand.

9.11.2. Updateschema virusdatabase

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.



Elementaire planning van updates voor de virusdatabase wordt beheerd met het onderdeel [Updatebeheer](#). In dat dialogvenster kunt u gedetailleerde parameters instellen voor het updateschema. In het tekstveld **Naam** (bij alle standaardschema's uitgeschakeld) staat de naam die door de leverancier van het programma aan het schema is toegewezen.

Schema wordt uitgevoerd

In dit gedeelte geeft u de tijdsintervallen op waarmee het nieuwe virusdatabase-updateschema moet worden uitgevoerd. U kunt dat interval op verschillende manieren definiëren: als steeds terugkerende --update die na verloop van een bepaalde tijd (**Uitvoeren elke ...**) moet worden uitgevoerd, of als update die op een bepaalde datum en een bepaald tijdstip (**Uitvoeren op specifiek tijdstip ...**) moet worden uitgevoerd.



Geavanceerde schemaopties

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

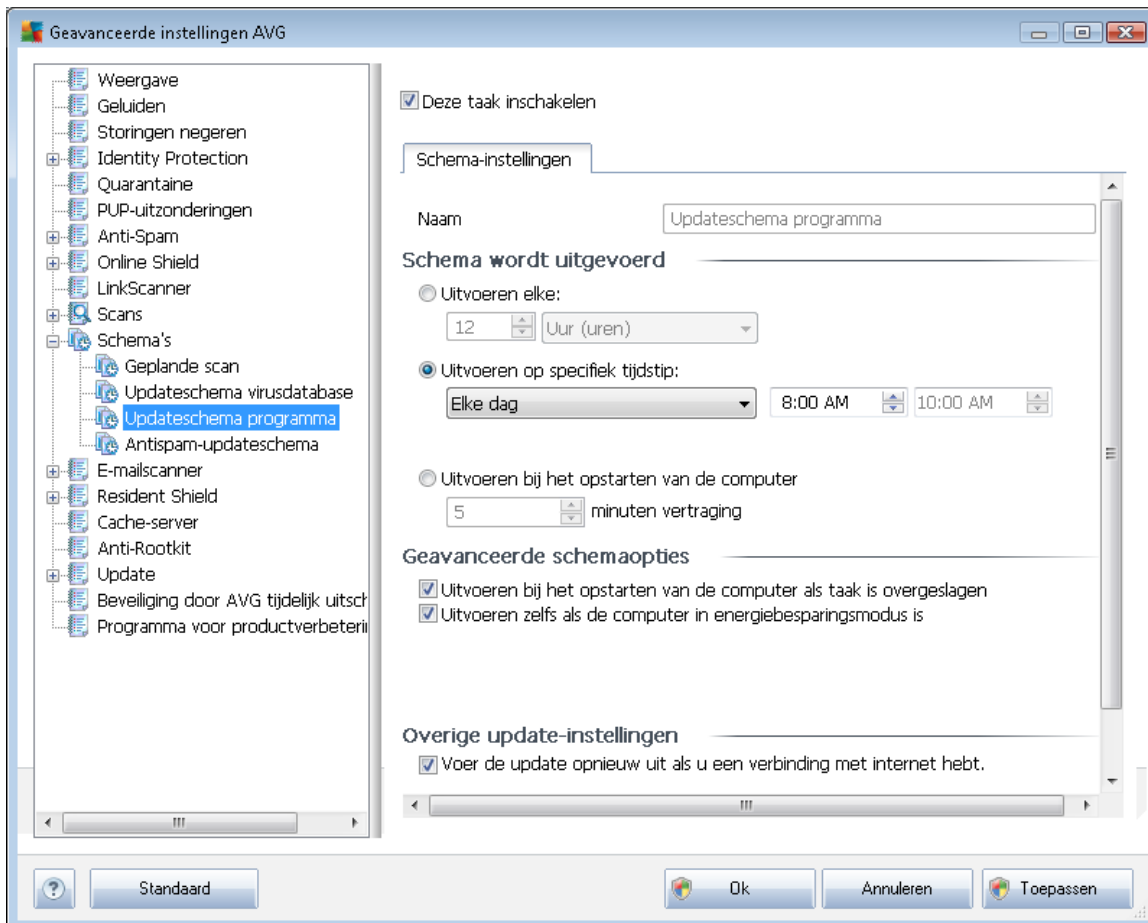
Overige update-instellingen

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

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

9.11.3. 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

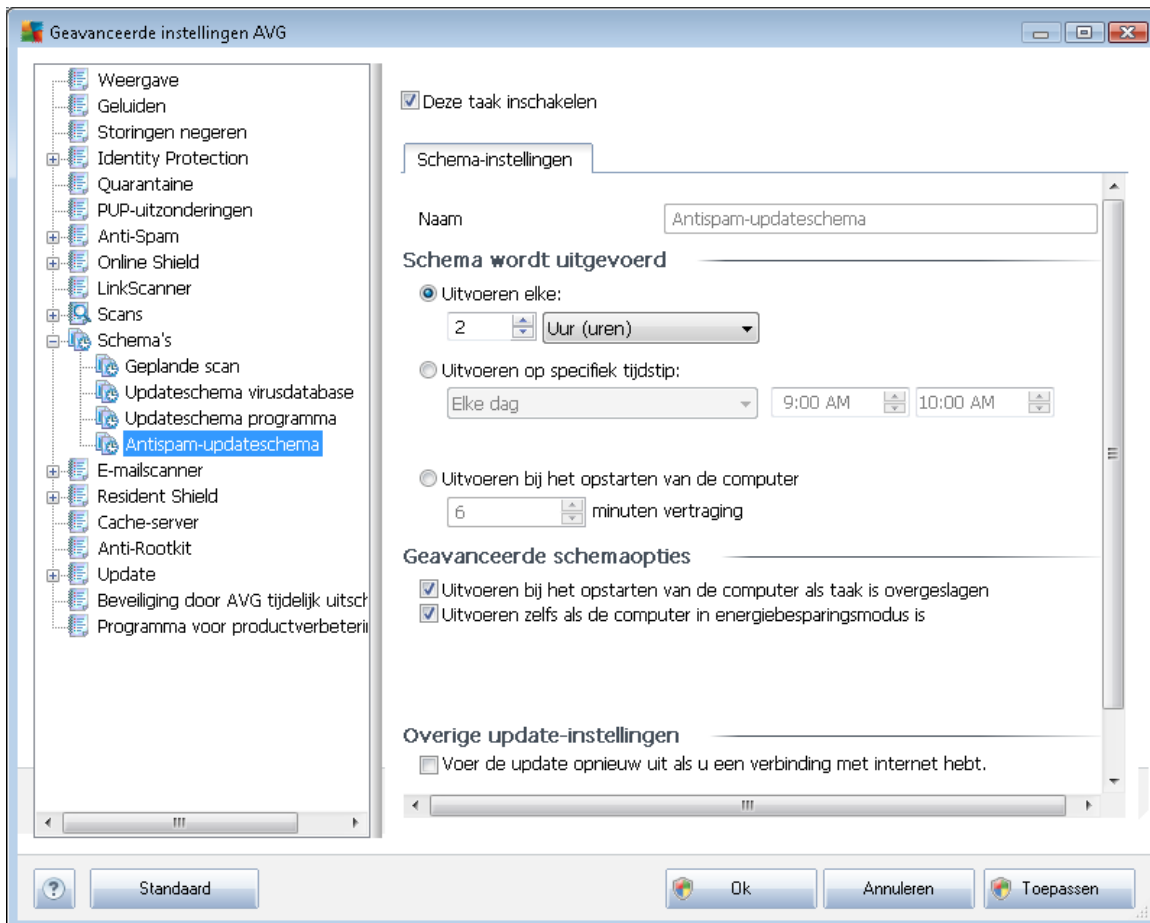
Schakel het selectievakje in bij **Voer de update opnieuw uit zodra de internetverbinding beschikbaar is** om ervoor te zorgen dat, als de internetverbinding verbroken wordt en de updateprocedure mislukt, die onmiddellijk weer opnieuw zal worden uitgevoerd na herstel van de internetverbinding.

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.

9.11.4. Antispam updateschema

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



Elementaire planning van **Anti-Spam**-updates wordt beheerd met het onderdeel **Updatebeheer**. In dat dialoogvenster kunt u gedetailleerde instellingen opgeven voor het updateschema. 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 het nieuwe **Anti-Spam**-updateschema moet worden uitgevoerd. U kunt deze interval op verschillende manieren definiëren: als steeds terugkerende **Anti-Spam**-update die na verloop van een bepaalde tijd (**Uitvoeren elke ...**) moet worden uitgevoerd, als update die op een bepaalde datum en een bepaald tijdstip (**Uitvoeren op specifiek tijdstip ...**) moet worden uitgevoerd, of door een gebeurtenis te definiëren waaraan het uitvoeren van de update moet worden gekoppeld (**Actie bij het opstarten van de computer**).



Geavanceerde schemaopties

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

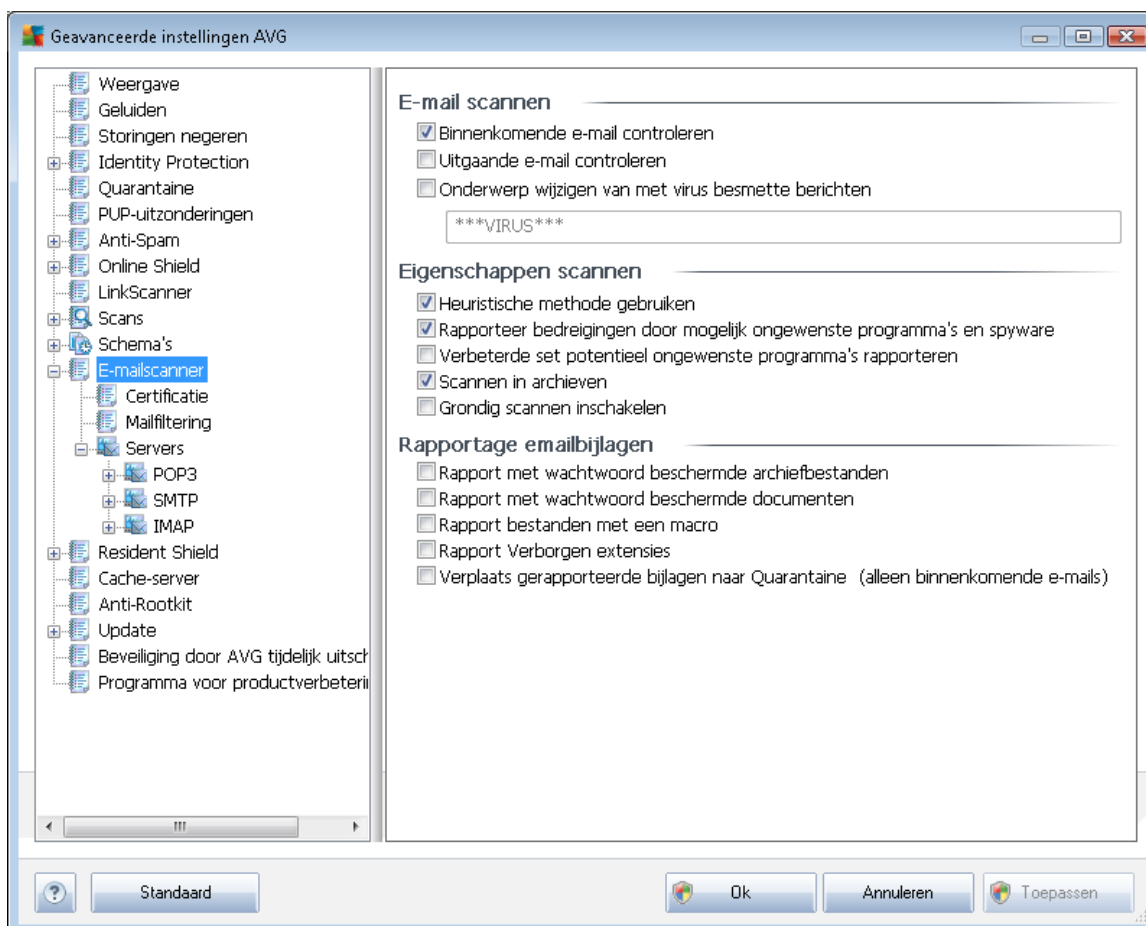
Overige update-instellingen

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

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

9.12. 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 geïnficeerd bericht** (*standaard uitgeschakeld*) – als u het selectievakje inschakelt, wordt u gewaarschuwd als er een geïnficeerd bericht is gedetecteerd. Die tekst zal dan worden toegevoegd aan de onderwerpregel van elk geïnficeerd 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

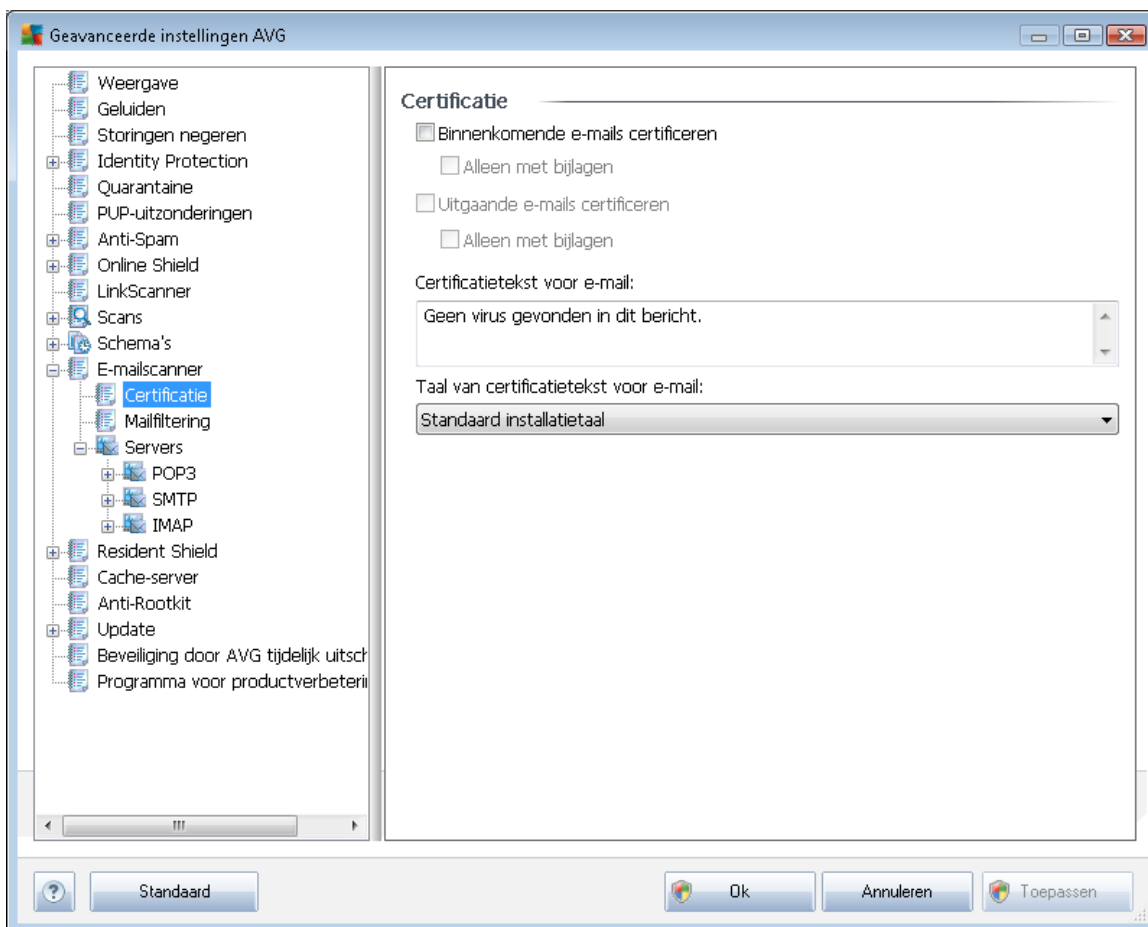
In dit gedeelte kunt u extra rapportages instellen omtrent potentieel gevaarlijke of verdachte bestanden. NB: er zal geen waarschuwingvenster worden weergegeven, er wordt alleen een certificeringstekst toegevoegd aan het eind van het e-mailbericht en al dergelijke rapporten worden vermeld in het dialoogvenster [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 vereenvoudigen (*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](#).

9.12.1. Certificatie

In het dialoogvenster **Certificatie** kunt u de tekst en de taal opgeven voor de certificaten in binnenkomende en uitgaande e-mail:





De tekst van het certificaat bestaat uit twee delen, het gebruikersgedeelte en het systeemgedeelte - zie het volgende voorbeeld: de eerste regel is het gebruikersgedeelte, de rest wordt automatisch gegenereerd:

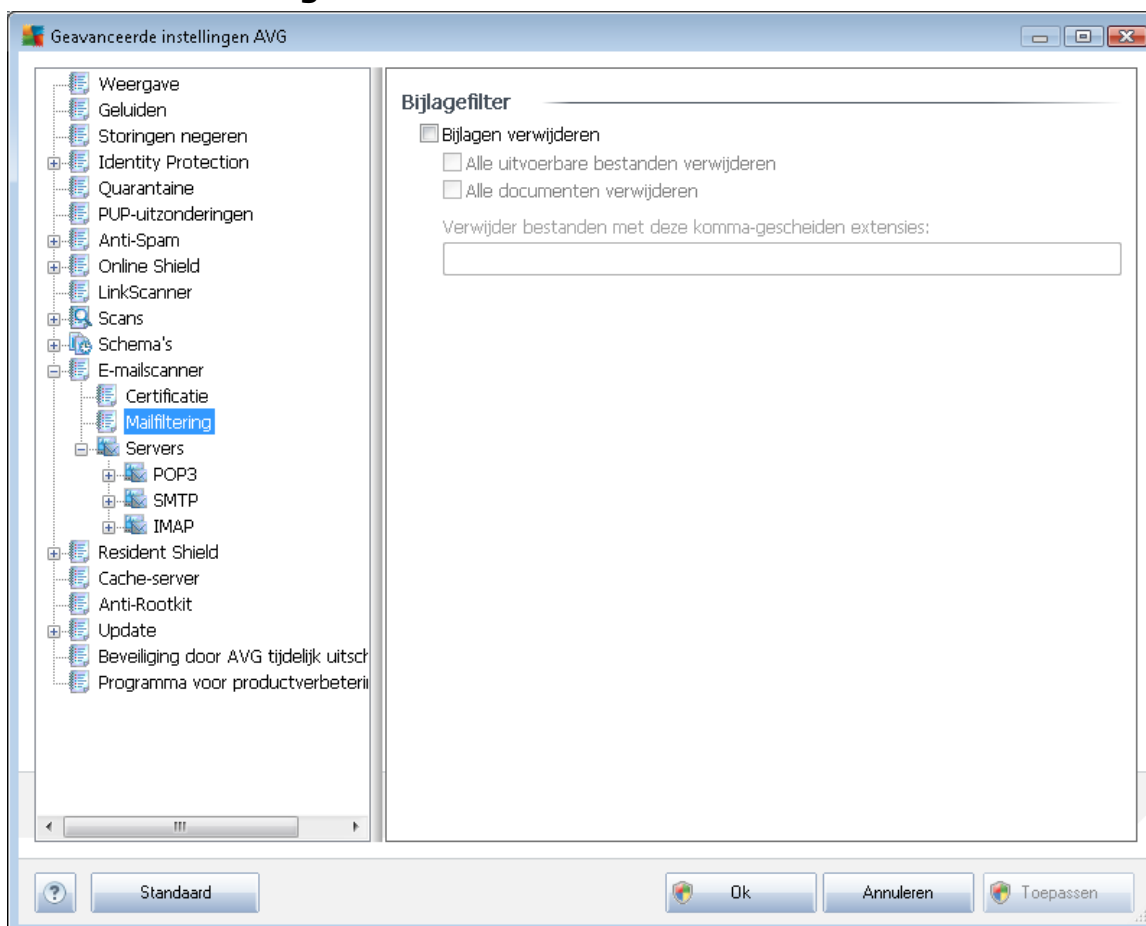
Geen virus gevonden in dit bericht.

Gecontroleerd door AVG.

Versie: x.y.zz / Virusdatabase: xx.y.z - datum van uitgifte: 12/9/2010

Als u besluit certificaten op te nemen in binnenkomende en uitgaande e-mail, kunt u in dit dialoogvenster de tekst opgeven voor het gebruikersgedeelte (**E-mailcertificatietekst**) en de taal opgeven voor het gedeelte dat automatisch wordt gegenereerd (**Taal voor e-mailcertificatietekst**).

9.12.2. Mailfiltering

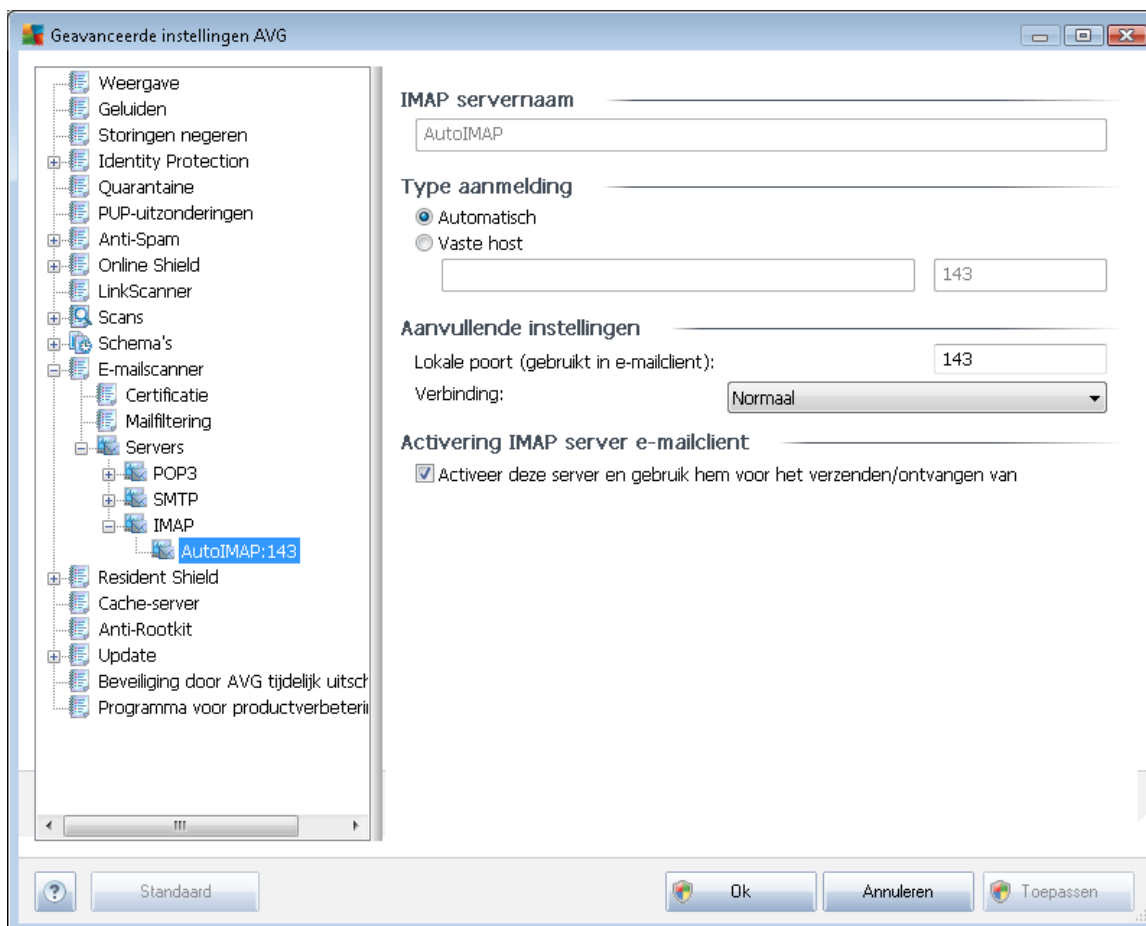


In het dialoogvenster **Bijlagefilter** kunt u parameters instellen voor het scannen van bijlagen bij e-mailberichten. Standaard is de optie **Bijlagen verwijderen** uitgeschakeld. Als u besluit die functie in te schakelen, worden alle bijlagen bij e-mailberichten die worden herkend als geïnfecteerd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

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

9.12.3. Servers

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

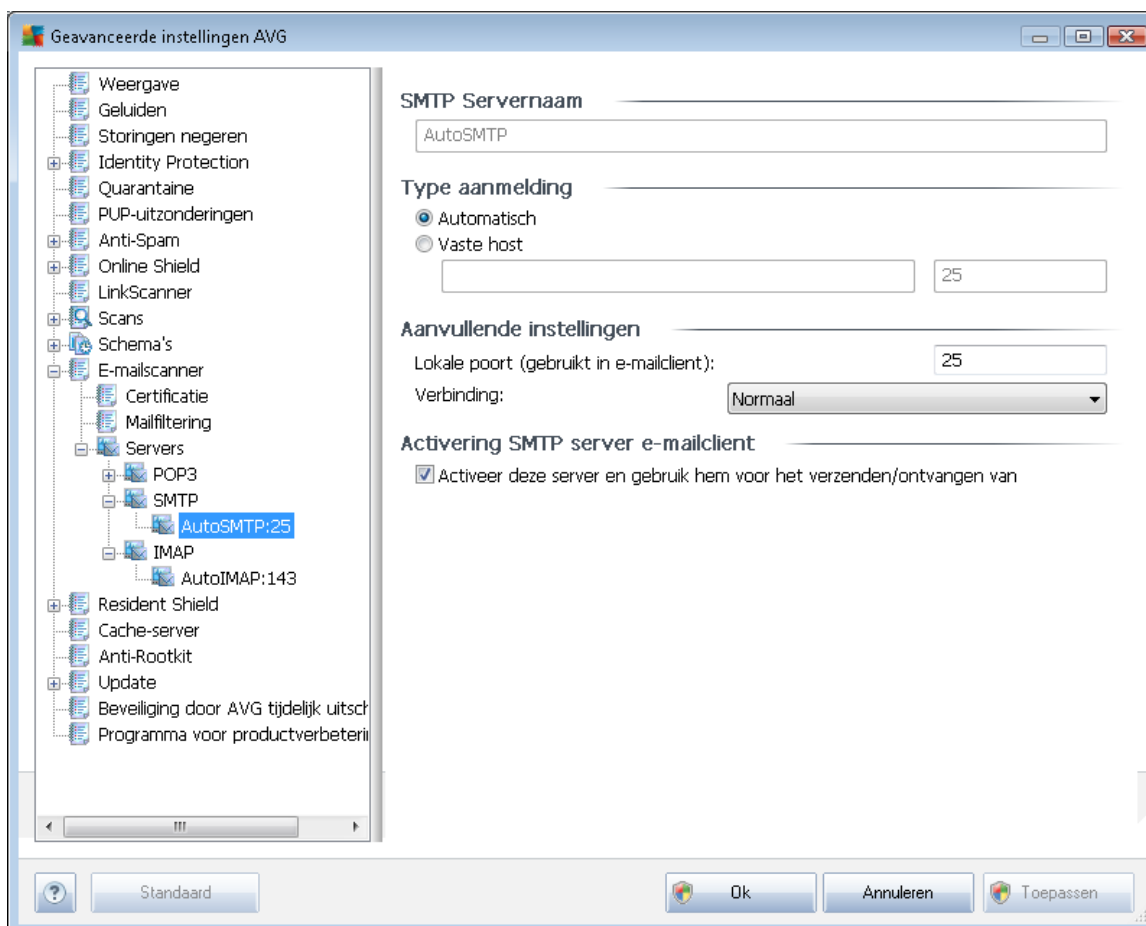


In dit dialoogvenster (geopend met **Servers / POP3**) kunt u een nieuwe [E-mailscanner](#)-server instellen die gebruikmaakt van het POP3-protocol voor binnenkomende e-mail:

- **POP3-servernaam** – 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 mailservers 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 mailservers 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 mailservers 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

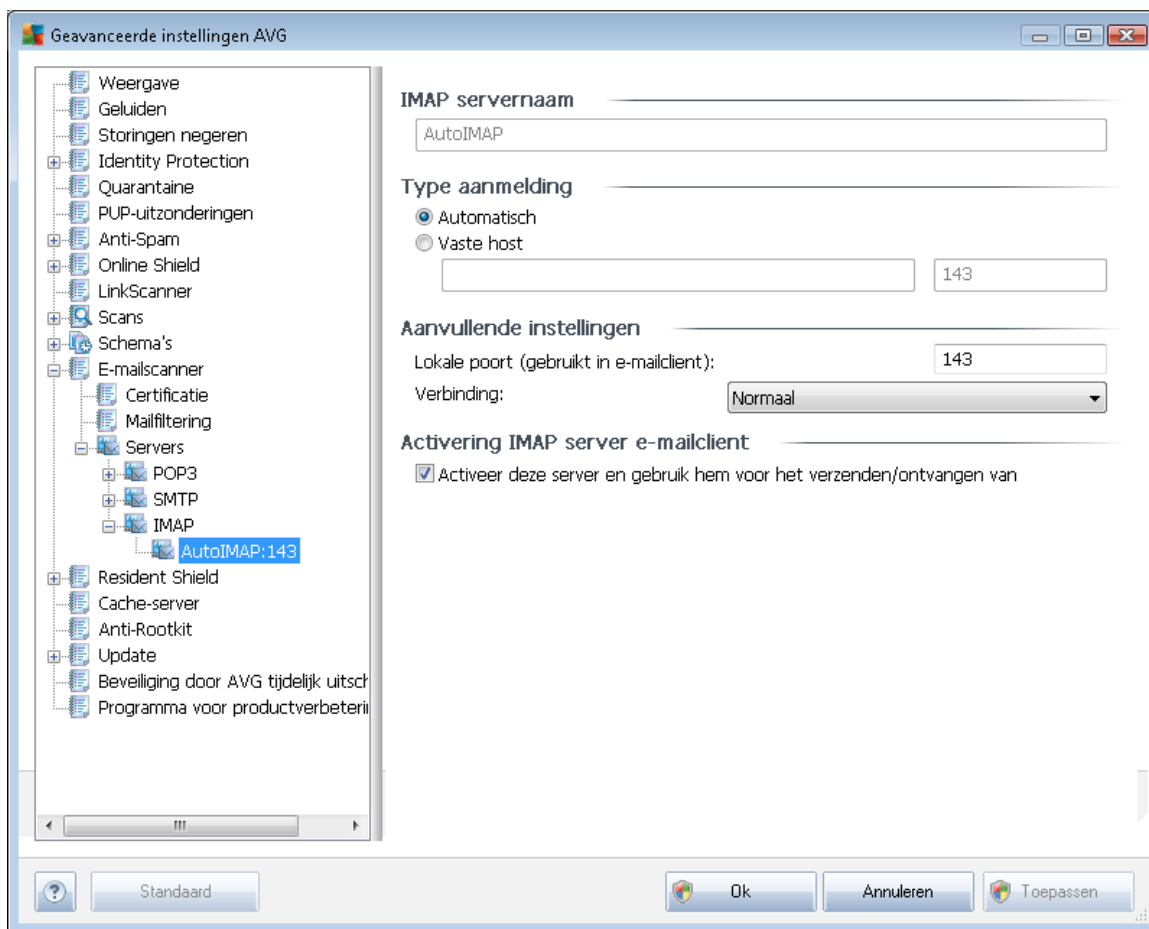


In dit dialoogvenster (geopend met **Servers / SMTP**) kunt u een nieuwe server instellen voor [E-mailscanner](#) die gebruikmaakt van het SMTP-protocol voor uitgaande e-mail:

- **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:

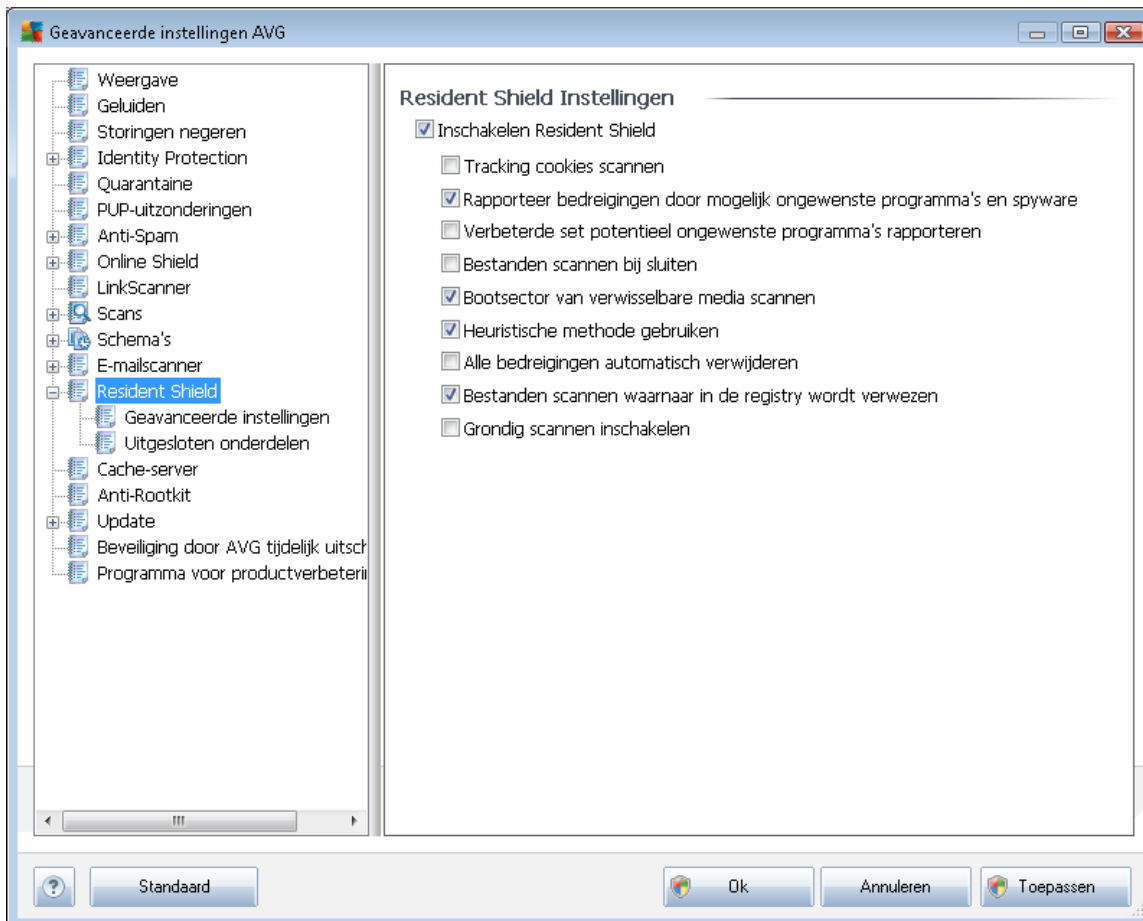
- **IMAP-servernaam** – in dit veld kunt u de naam opgeven van nieuwe servers (*als u een*

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 mailservers 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 mailservers op. U kunt een domeinnaam gebruiken (*bijvoorbeeld smtp.acme.com*), maar ook een IP-adres (*bijvoorbeeld 123.45.67.89*). *Als de mailservers een niet-standaard poort gebruikt, kunt u deze poort na de servernaam opgeven. Gebruik een dubbele punt als scheidingstekens (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 welke 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

9.13. Resident Shield

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



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

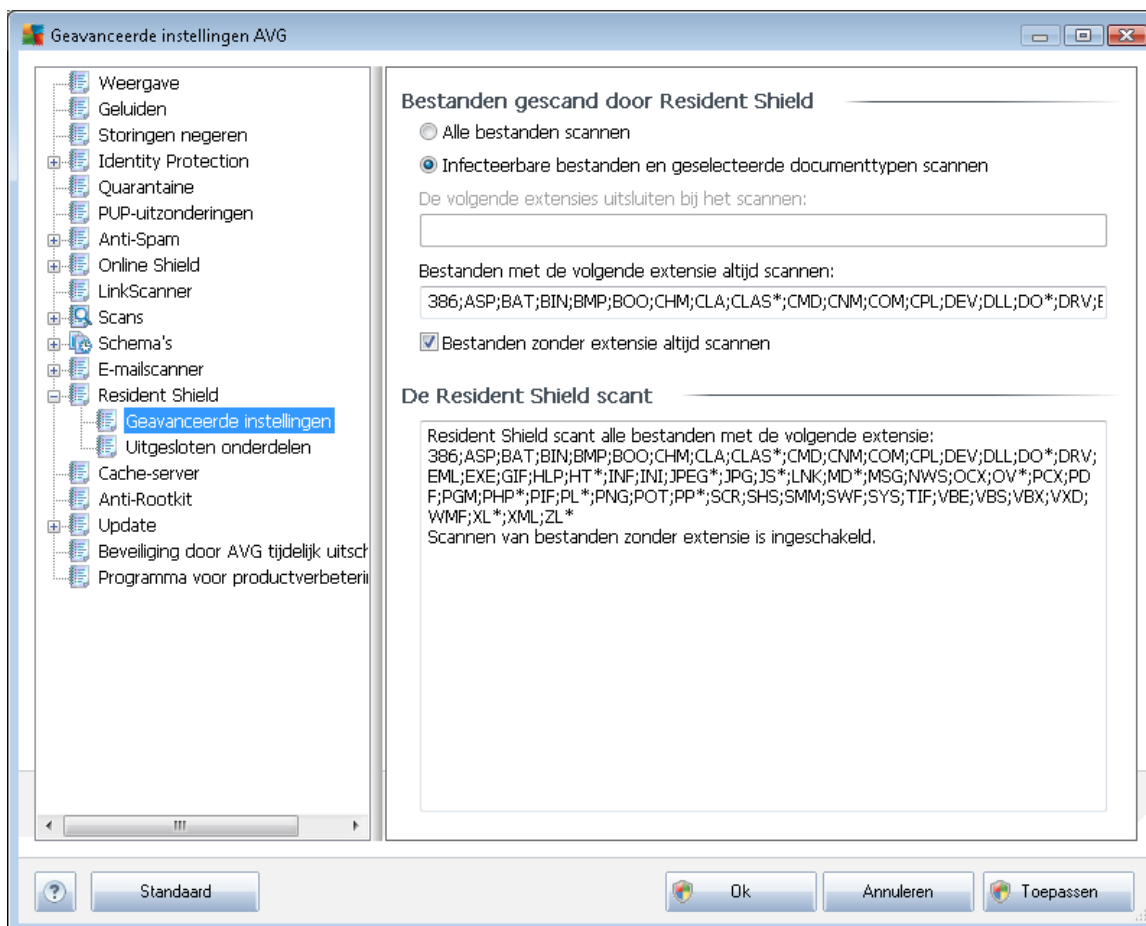
- **Tracking cookies scannen** – deze parameter geeft aan of u cookies wilt opsporen tijdens het scannen. (HTTP-cookies worden gebruikt voor verificatie, tracking en het bijhouden van bepaalde informatie over gebruikers, bijvoorbeeld voorkeuren voor websites of de inhoud van winkelkarretjes)
- **Bedreigingen door mogelijk ongewenste programma's en spyware rapporteren** (standaard ingeschakeld) – schakel dit selectievakje in om de **Anti-Spyware**-engine te activeren en naar spyware en virussen te scannen. [Spyware behoort tot een twijfelachtige categorie malware: 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.
- **Bestanden scannen bij sluiten** (standaard uitgeschakeld) – scannen bij afsluiten zorgt ervoor dat actieve objecten (bijv. toepassingen, documenten, enz.) worden gescand als ze worden geopend en gesloten; de functie levert een bijdrage aan de bescherming tegen bepaalde geavanceerde virustypen
- **Bootsector van verwisselbare media scannen** (standaard ingeschakeld)
- **Heuristische methode gebruiken** (standaard ingeschakeld) – [heuristische analyse](#) (dynamische emulatie van de instructies van gescande objecten in een virtuele computeromgeving) wordt gebruikt als één van de methoden voor virusdetectie
- **Alle bedreigingen automatisch verwijderen** (standaard uitgeschakeld) – gedetecteerde infecties worden automatisch hersteld als dat kan, alle infecties die niet kunnen worden hersteld worden automatisch verwijderd.
- **Bestanden scannen waarnaar wordt verwezen in het register** (standaard ingeschakeld) – AVG scant alle uitvoerbare bestanden die worden toegevoegd aan het opstartregister om te voorkomen dat een bekende infectie bij een volgende keer starten van de computer wordt uitgevoerd.
- **Grondig scannen inschakelen** (standaard uitgeschakeld) – onder bepaalde omstandigheden (*in extreme noodgevallen*) kunt u deze optie inschakelen om de meest grondige algoritmes te activeren, waarmee elk mogelijk bedreigend object tot diep in het systeem wordt onderzocht. Deze manier van scannen kost echter erg veel tijd.

9.13.1. Geavanceerde instellingen

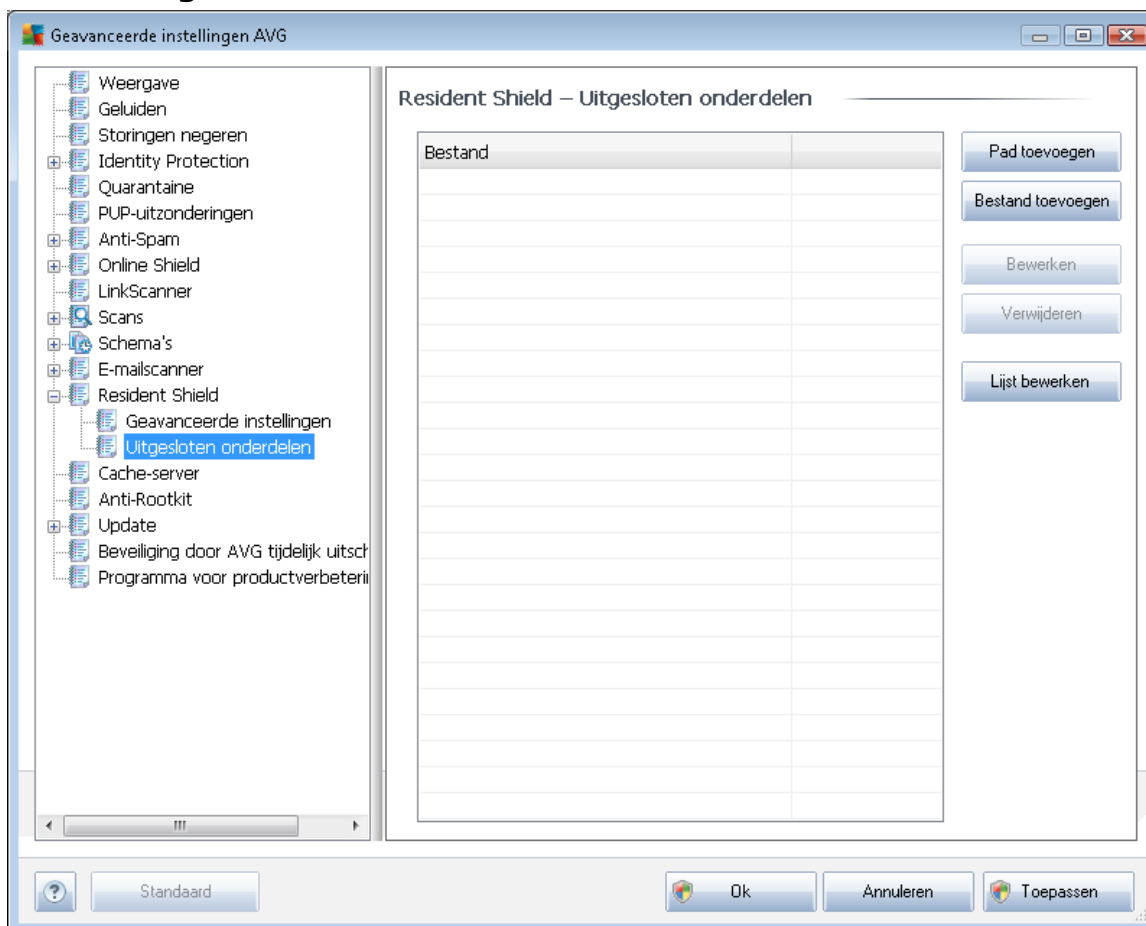
In het dialoogvenster **Bestanden gescand door Resident Shield** kunt u opgeven welke bestanden gescand moeten worden (*aan de hand van de extensies*):



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

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

9.13.2. Uitgesloten onderdelen



In het dialoogvenster **Resident Shield – uitsluitingen** 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!

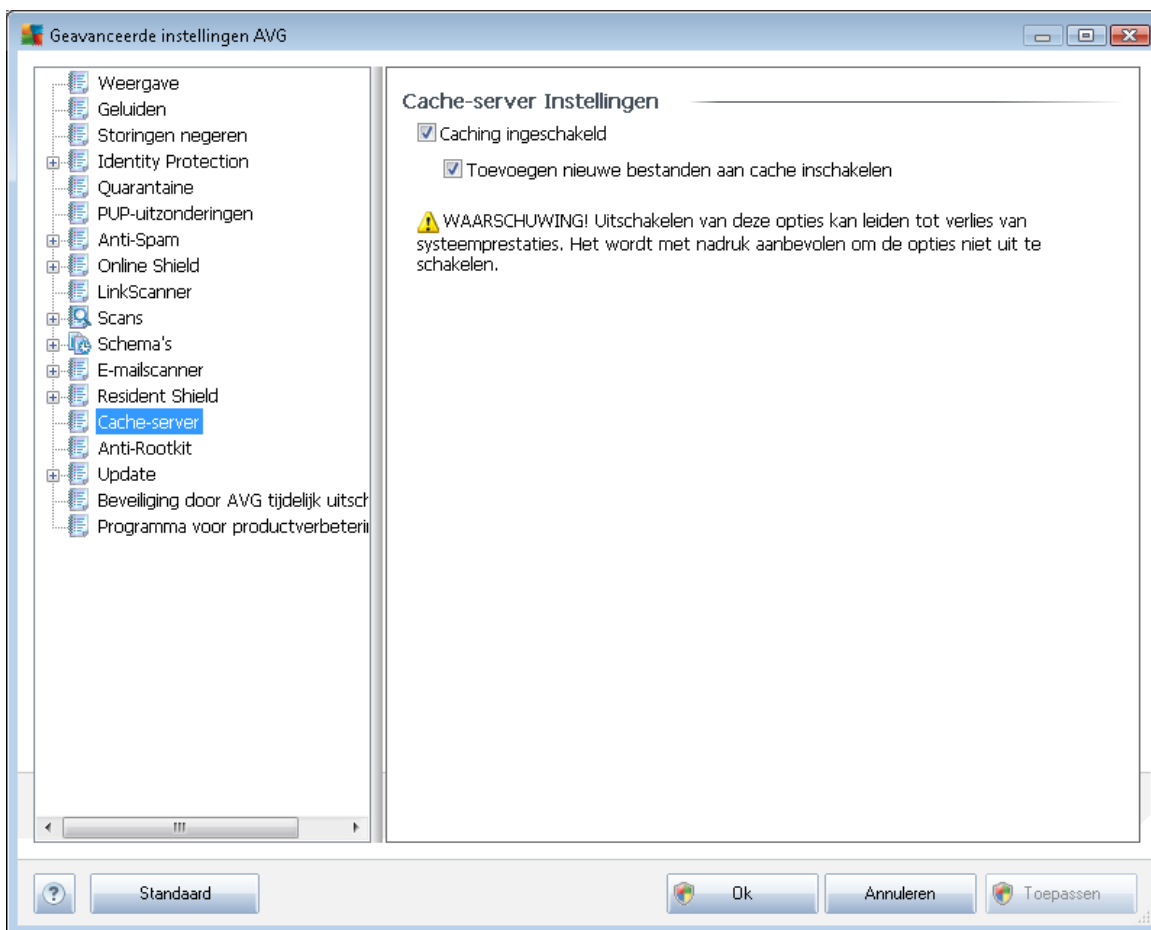
Dit dialoogvenster heeft de volgende knoppen:

- **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

9.14. Cacheserver

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



In dit dialoogvenster kunt u uit twee instellingen kiezen:

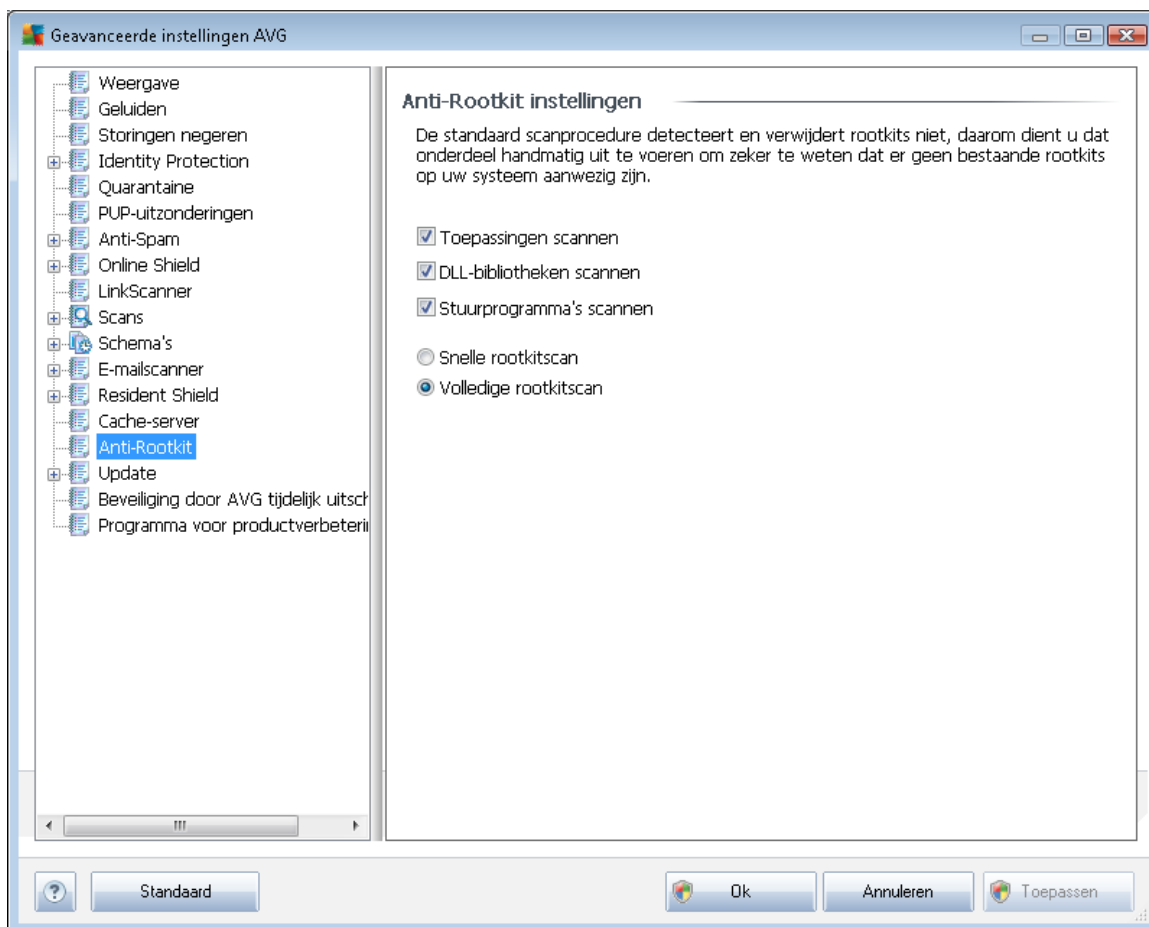
- **Caching ingeschakeld** (*standaard ingeschakeld*) - schakel het selectievakje uit om de **Cache-server** uit te schakelen en het cachegeheugen te legen. Let op: het scannen kan trager verlopen, en de prestaties van de computer kunnen te wensen over laten, omdat elk afzonderlijk bestand dat wordt gebruikt, eerst moet worden gescand op virussen en spyware.
- **Toevoegen nieuwe bestanden aan cache inschakelen** (*standaard ingeschakeld*) - schakel dit selectievakje uit om te verhinderen dat nog meer bestanden worden toegevoegd aan het cachegeheugen. Alle bestanden die al zijn opgeslagen in de cache, blijven daar totdat het cachen helemaal wordt uitgeschakeld, of tot de eerstvolgende update van de



virusdatabase.

9.15. Antirootkit

In dit dialoogvenster kunt u de configuratie van het onderdeel [Anti-rootkit](#) bewerken:



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

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

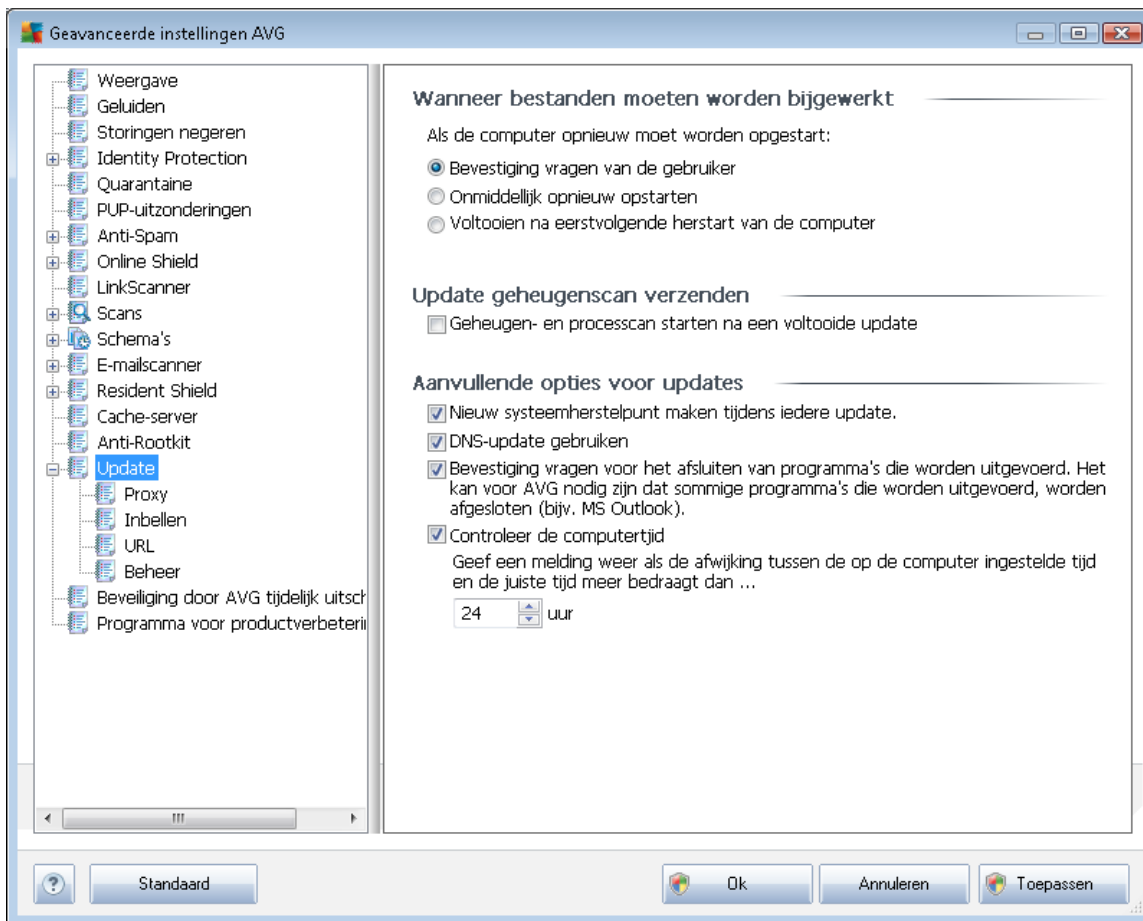
- **Toepassingen scannen**
- **DLL-bibliotheken scannen**
- **Stuurprogramma's scannen**

Vervolgens kunt u de scanmodus kiezen:

- **Snelle rootkitscan** – 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 systeemap (standaard *c:\Windows*) plus alle locale schijven (*inclusief flash-stations, maar exclusief diskette-/cd-stations*)

9.16. Update



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

Wanneer bestanden moeten worden bijgewerkt

In dit gedeelte kunt u een keuze maken uit drie alternatieven als het updateproces een herstart van de computer vereist. Het voltooiën 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** (standaard) – u wordt gevraagd een herstart te bevestigen die nodig is voor het voltooiën van de [updateprocedure](#)
- **Onmiddellijk opnieuw opstarten** – de computer wordt automatisch opnieuw gestart nadat de [updateprocedure](#) is voltooid, u hoeft daarvoor geen toestemming meer te verlenen



- **Voltooien na eerstvolgende herstart van de computer** – het voltooien van het [updateproces](#) wordt uitgesteld tot de eerstvolgende herstart van de computer. Deze optie wordt alleen aanbevolen als u de computer regelmatig opnieuw opstart, minstens één keer per dag.

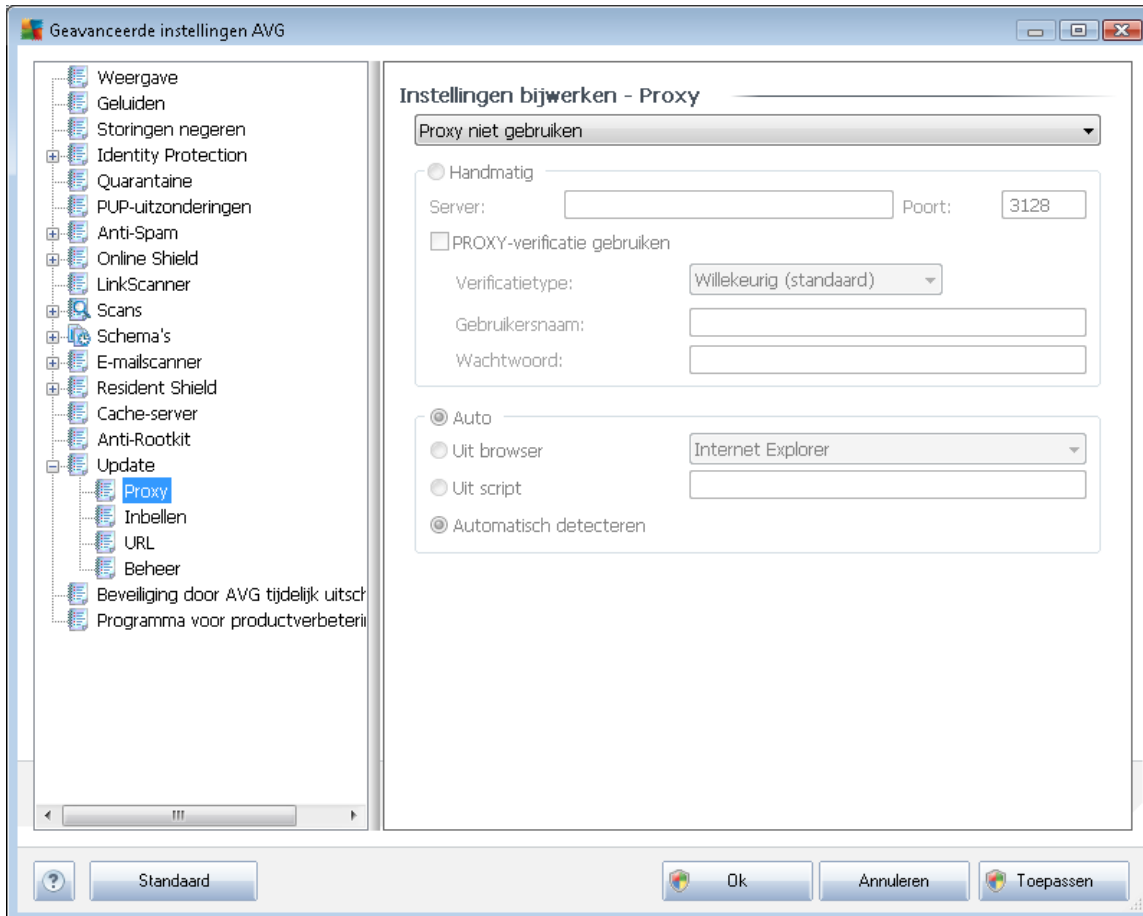
Update geheugenscan verzenden

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 Internet Security 2011** 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 om actieve toepassingen te sluiten (standaard ingeschakeld)** – deze optie zorgt ervoor dat u zeker weet dat er geen toepassingen die worden uitgevoerd, zullen worden afgesloten zonder uw expliciete toestemming – mocht dat afsluiten nodig zijn voor het voltooien van de updateprocedure;
- **Controleer de computertijd** – schakel deze optie in om aan te geven dat u er van op de hoogte wilt worden gesteld als de computertijd afwijkt van de juiste tijd met meer dan een opgegeven aantal uren.

9.16.1. Proxy



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

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

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

Handmatige configuratie

Als u kiest voor handmatige configuratie (schakel *het selectievakje* **Handmatig** in om het



desbetreffende deel van het dialoogvenster te activeren), specificieert 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*)

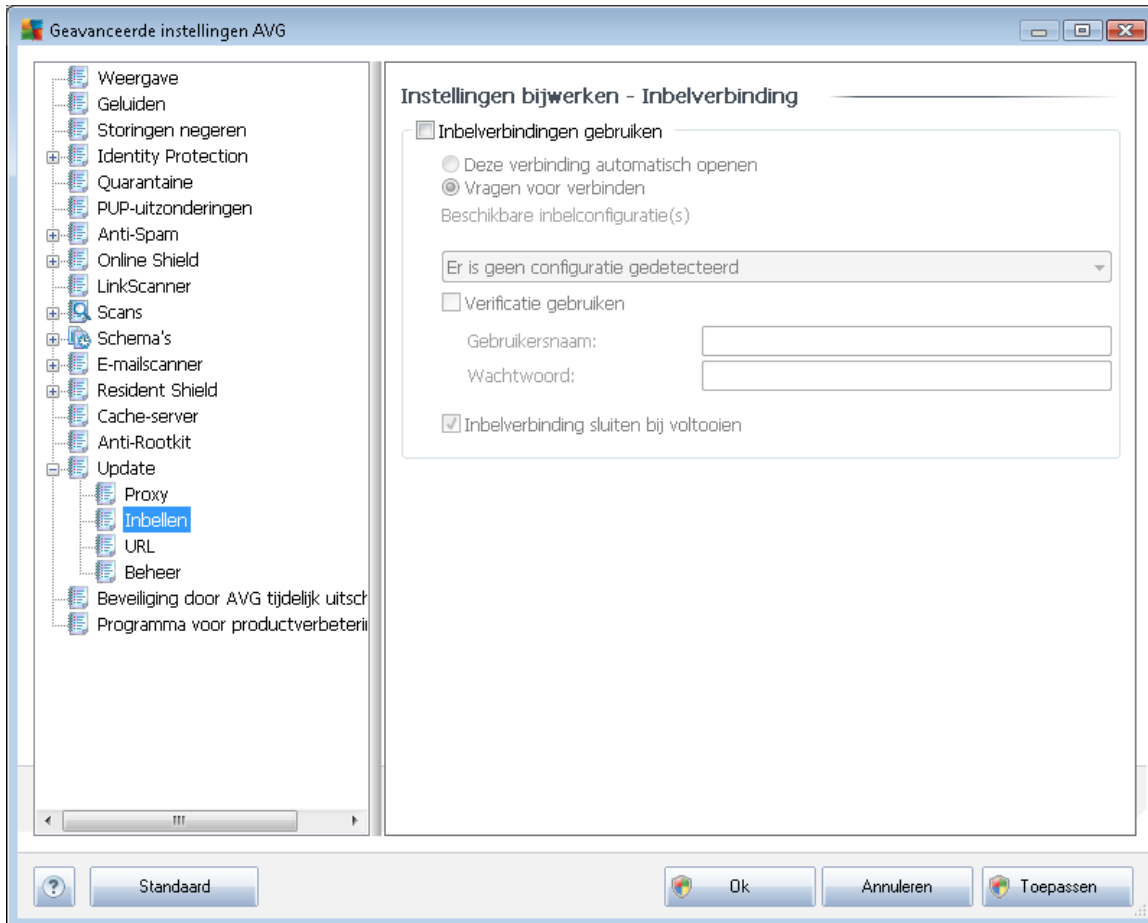
Het is mogelijk op de proxyserver voor de afzonderlijke gebruikers verschillende regels in te stellen. Als dat voor uw proxyserver het geval is, schakelt u het selectievakje **PROXY-verificatie gebruiken** in om te controleren of uw gebruikersnaam en wachtwoord geldig zijn voor een verbinding met internet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

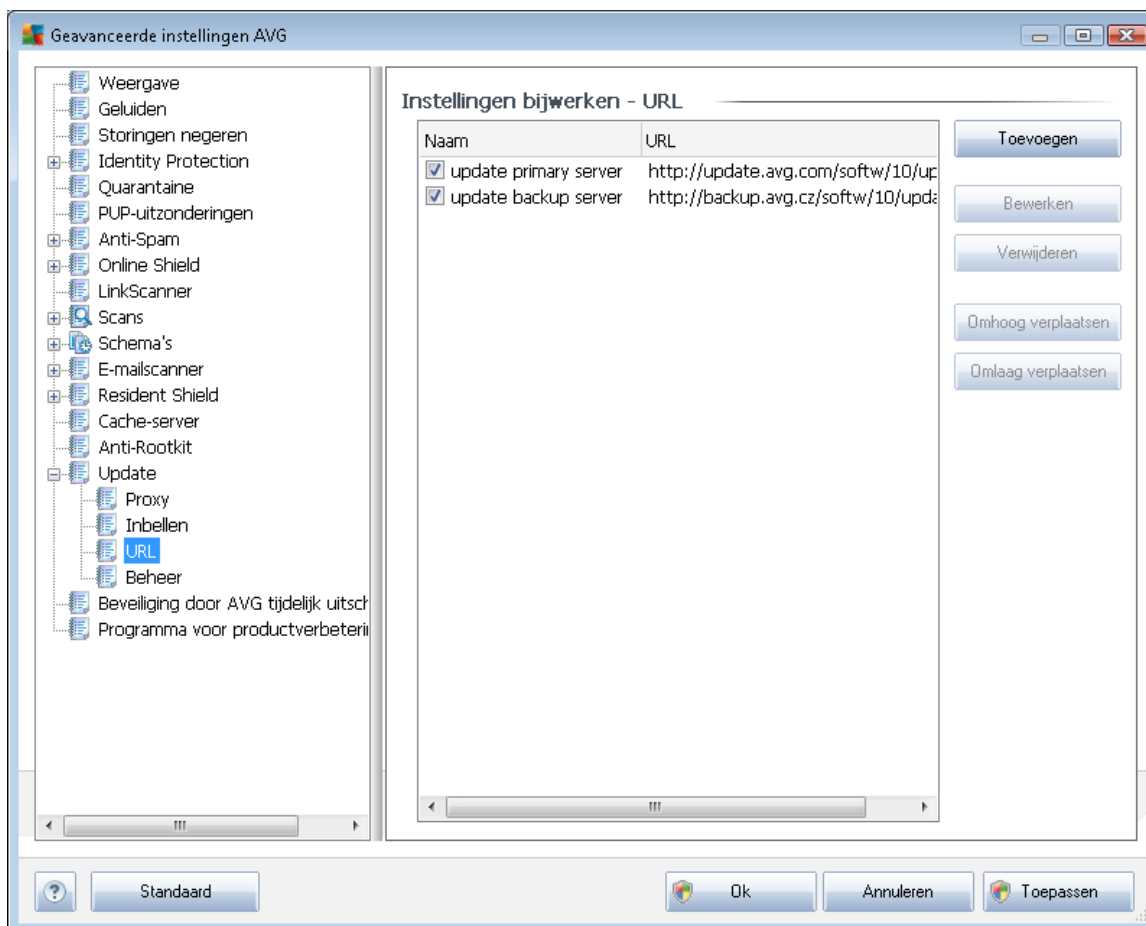
9.16.2. Inbellen



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

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

9.16.3. URL

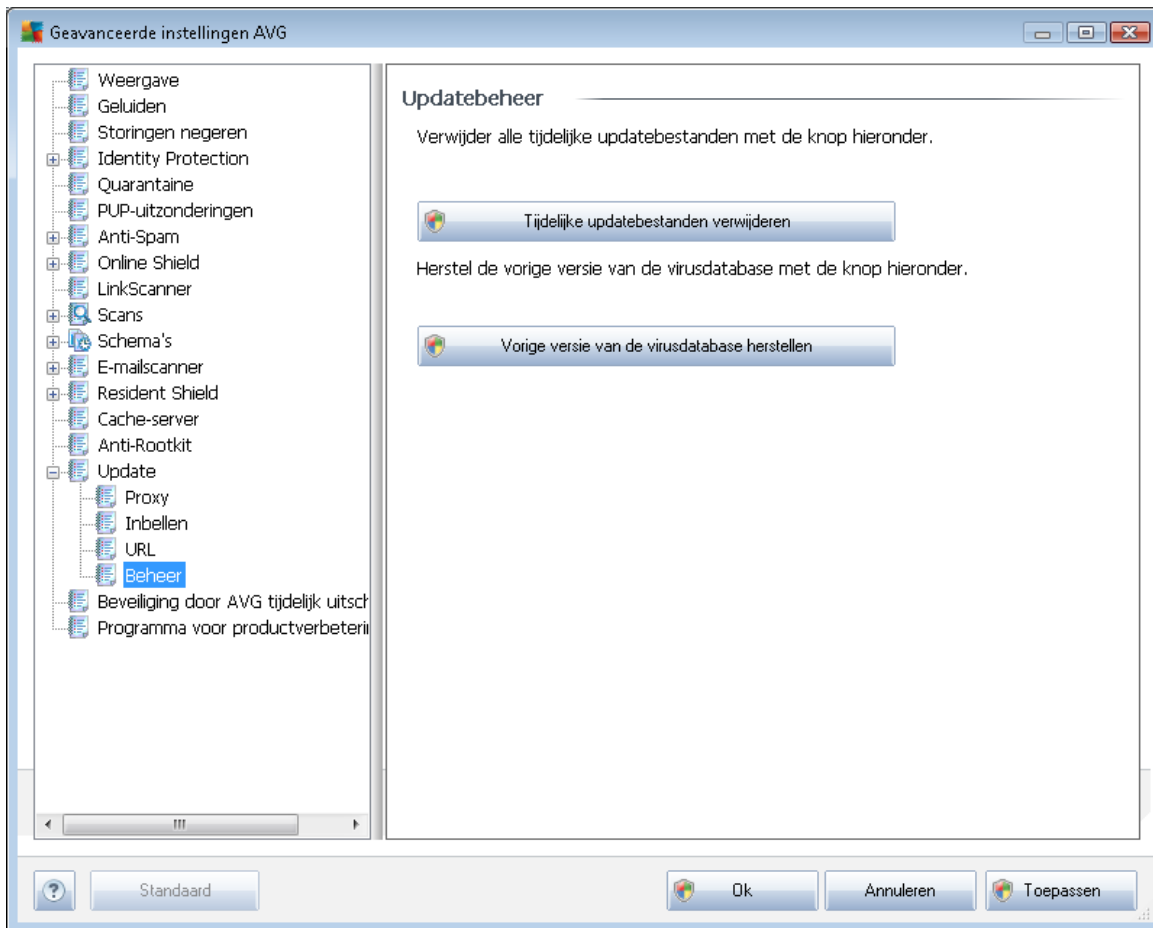


Op het tabblad **URL** wordt een lijst met internetadressen weergegeven die u kunt gebruiken om de updatebestanden te downloaden. De lijst en de vermeldingen kunnen worden gewijzigd met behulp van de volgende knoppen:

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

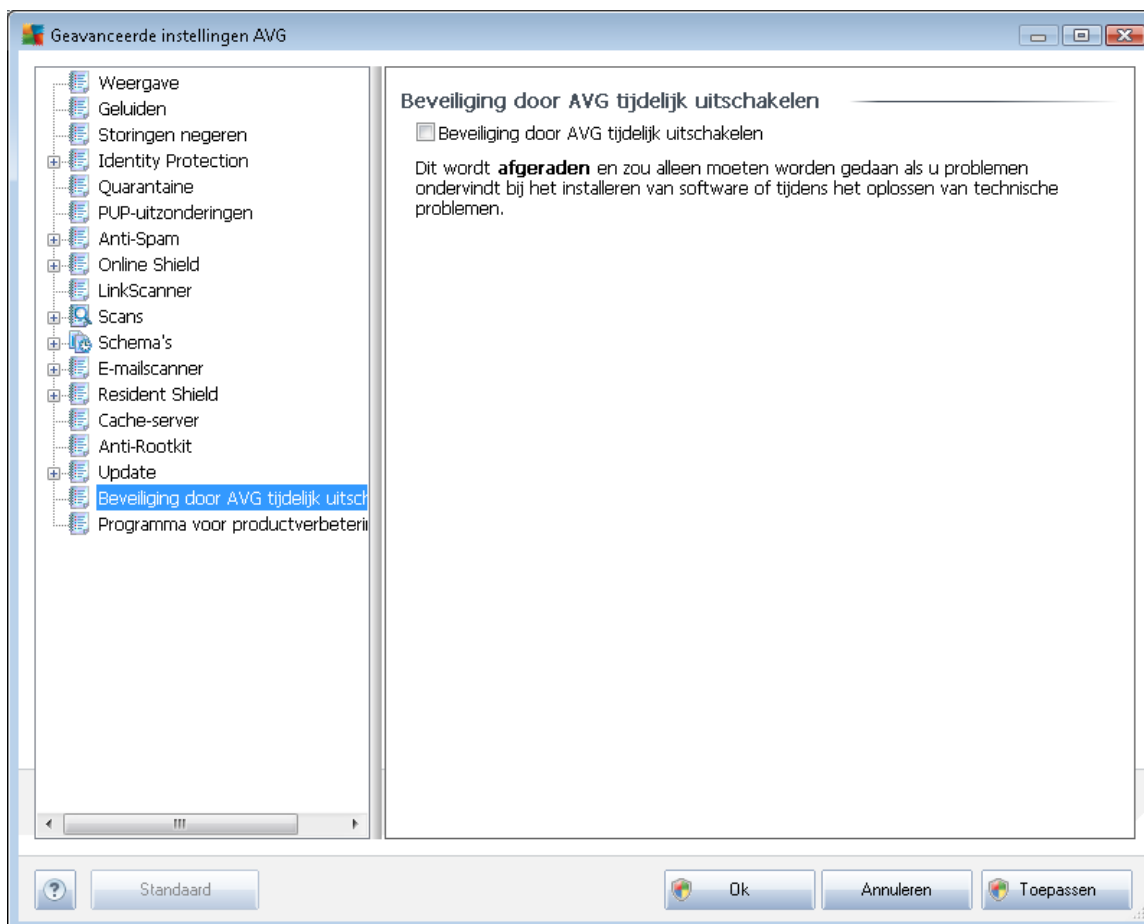
9.16.4. Beheer

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



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

9.17. AVG-bescherming tijdelijk uitschakelen



In het dialoogvenster **AVG-bescherming tijdelijk uitschakelen** kunt u de volledige bescherming door **AVG Internet Security 2011** in één keer uitschakelen.

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

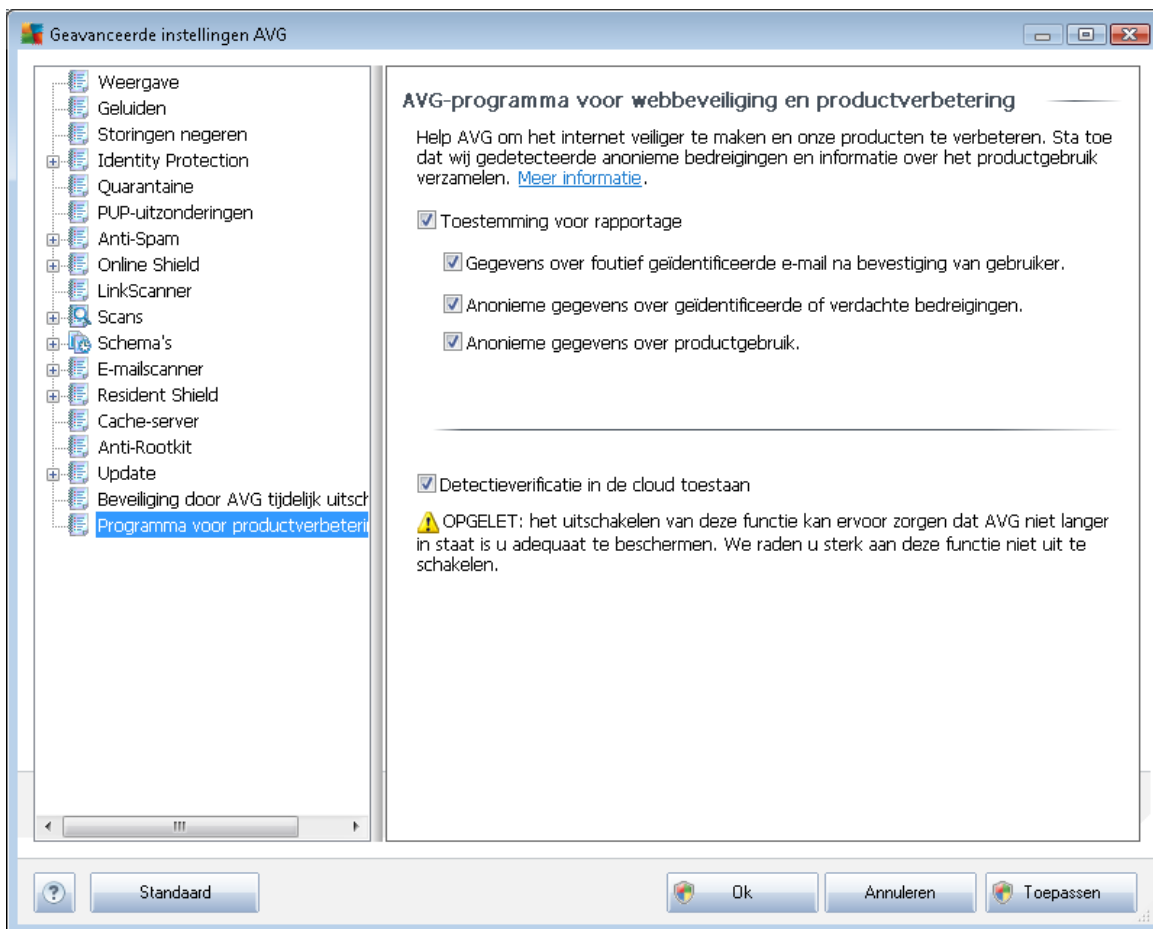
In de meeste gevallen is het **niet nodig** om AVG uit te schakelen voordat u nieuwe software installeert, zelfs niet als het installatieprogramma of de softwarewizard voorstelt eerst lopende programma's en toepassingen uit te schakelen om ervoor te zorgen dat er zich geen ongewenste onderbrekingen voordoen tijdens het installatieproces. Probeer het eerst alleen door **Resident Shield** uit te schakelen als er werkelijk problemen ontstaan tijdens een installatie. Als het nodig is om AVG tijdelijk uit te schakelen, dient u de bescherming zo snel mogelijk weer in te schakelen. Uw computer is kwetsbaar en kan worden aangevallen als u verbonden bent met internet of een netwerk gedurende de tijd dat uw bescherming is uitgeschakeld.

9.18. Programma voor productverbetering

Het dialoogvenster **AVG-programma voor internetveiligheid en productverbetering** is een uitnodiging deel te nemen aan productverbetering door AVG en ons te helpen de algehele veiligheid op internet te vergroten. Schakel de optie **Rapportage toestaan** 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 bescherming bieden.

De rapportage vindt automatisch plaats en u hebt er dus geen last van. Er wordt geen persoonlijke informatie in de rapportage opgenomen. Rapportage van gedetecteerde bedreigingen is optioneel, maar we vragen u deze functie ook in te schakelen omdat het ons helpt de online surfbescherming te verbeteren voor zowel u als andere AVG-gebruikers.



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, 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; het stuurt zichzelf zelfstandig door naar andere computers, gewoonlijk via e-mail, en zorgt zo vaak voor 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 mogelijkereis 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.
- Оок **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.
- Еєν **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 spammiltje 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.

Om u te beschermen tegen al deze verschillende soorten bedreigingen heeft AVG de volgende onderdelen:

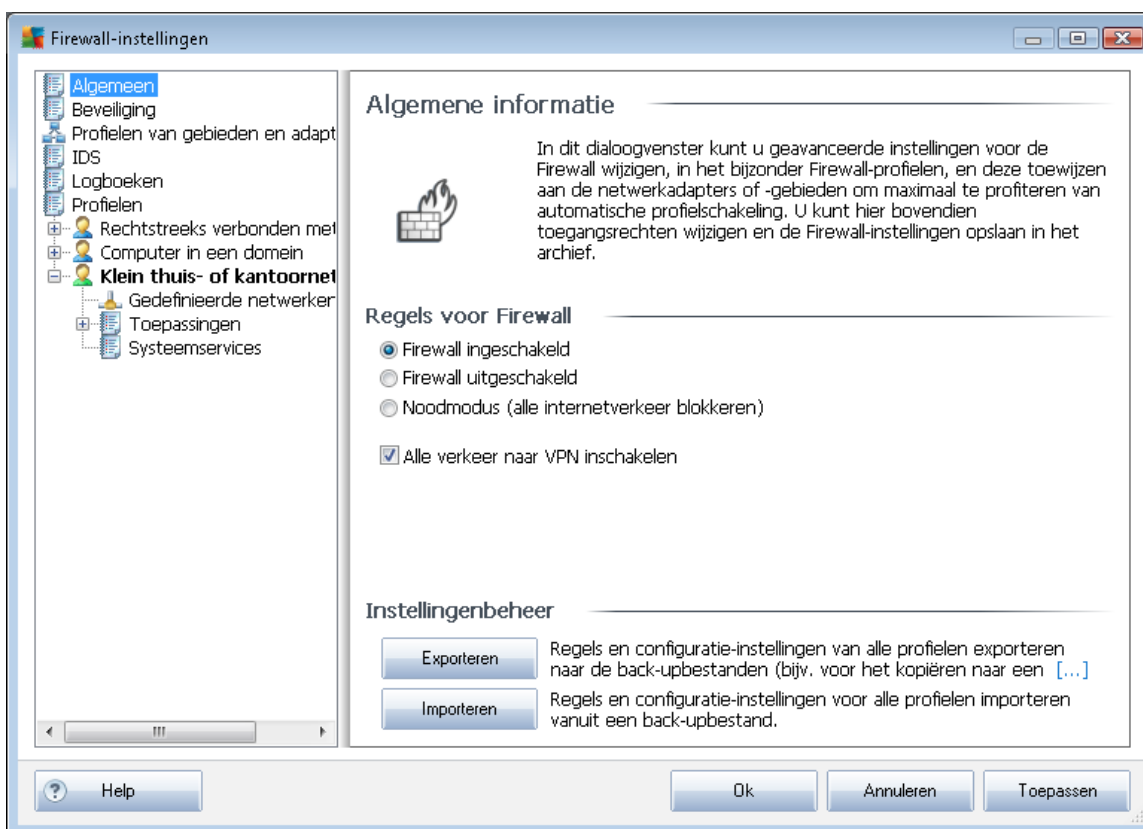
- **Anti-Virus** om uw computer tegen virussen te beschermen,
- **Anti-Spyware** om uw computer tegen spyware te beschermen,
- **Online Shield** om u te beschermen tegen zowel virussen als spyware, als u op het internet surft,
- **LinkScanner** om u te beschermen tegen andere online bedreigingen die in dit hoofdstuk worden genoemd.

10. Firewallinstellingen

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

10.1. Algemeen

Het dialoogvenster **Algemene informatie** is verdeeld in twee secties:



Firewallstatus

In het gedeelte **Firewallstatus** kunt u de status van **Firewall** aanpassen aan de omstandigheden:

- **Firewall ingeschakeld** – selecteer deze optie om communicatie toe te staan aan die toepassingen waarvoor 'toegestaan' is ingesteld in de set regels gedefinieerd voor het geselecteerde **Firewallprofiel**
- **Firewall uitgeschakeld** – met deze optie schakelt u **Firewall** helemaal uit; alle netwerkverkeer is toegestaan en er wordt niet gecontroleerd!
- **Alarmmodus (al het internetverkeer blokkeren)** – met deze optie blokkeert u al het verkeer

via alle netwerkpoorten; **Firewall** is weliswaar actief, maar al het netwerkverkeer is stilgelegd

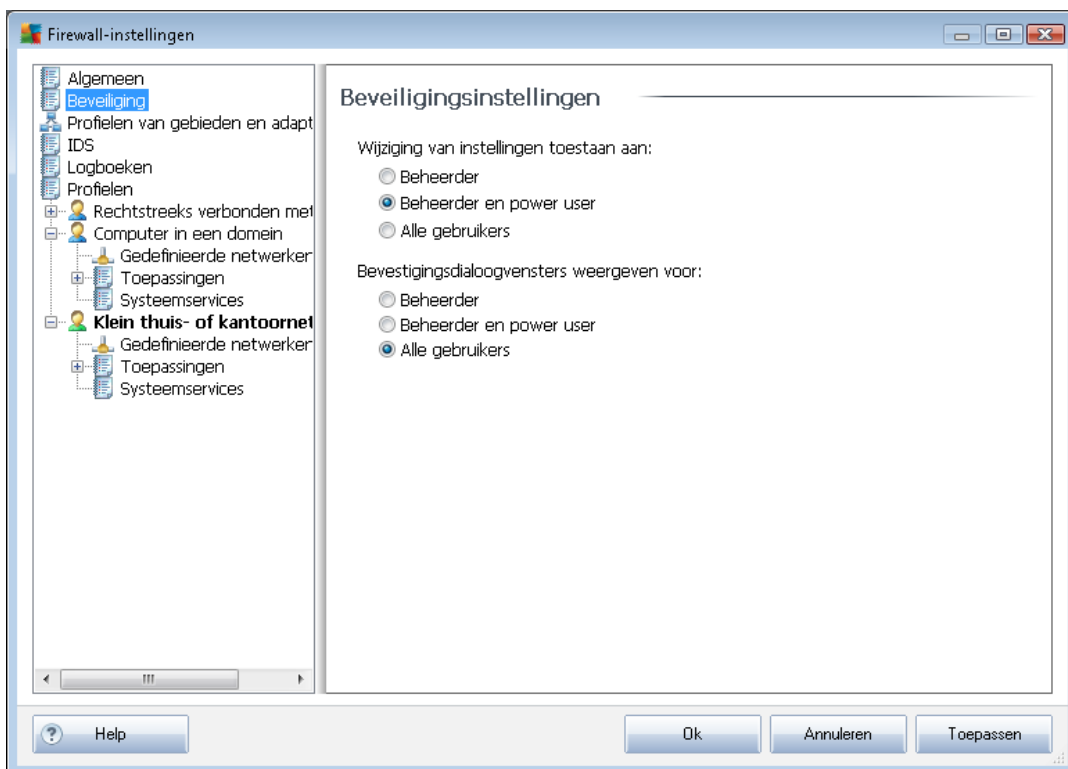
- **Alle verkeer naar VPN inschakelen** – als u gebruikmaakt van een VPN-verbinding (*Virtual Private Network*), bijvoorbeeld om u thuis aan te melden bij het kantoor netwerk, raden we u aan dit selectievakje in te schakelen. **AVG Firewall** zoekt automatisch de netwerkadapters die voor VPN-verbindingen worden gebruikt en staat alle toepassingen toe verbinding te maken met het doelnetwerk (*dit geldt alleen voor toepassingen waarvoor geen specifieke firewallregels zijn opgesteld*). In een standaardstelsel met gangbare netwerkadapters bespaart deze eenvoudige stap u het opstellen van een gedetailleerde regel voor elke toepassing die u via het VPN wilt gebruiken.

Opmerking: voor het inschakelen van een VPN-verbinding is het noodzakelijk communicatie toe te staan voor de volgende protocollen: GRE, ESP, L2TP, PPTP. Dat kunt u doen in het dialoogvenster *Systemservices*.

Instellingenbeheer

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

10.2. Beveiliging



In het dialoogvenster **Beveiligingsinstellingen** kunt u algemene regels opstellen voor de **Firewall**,

ongeacht het geselecteerde profiel:

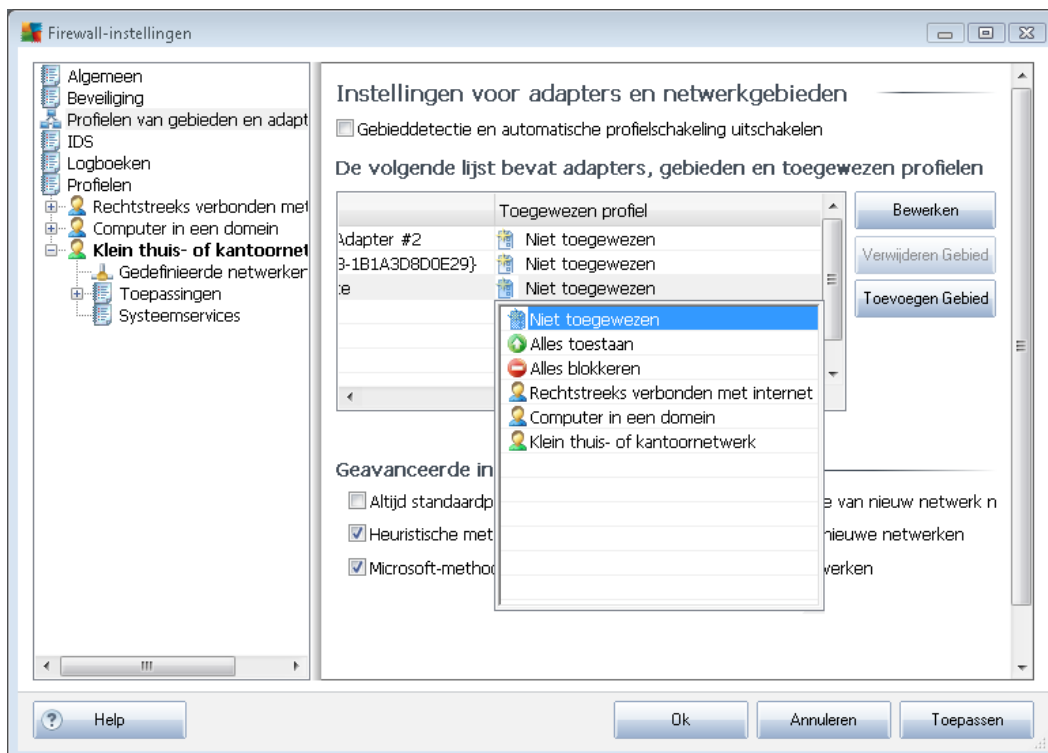
- **Wijzigingen toestaan door** - specificeren wie de configuratie van de **Firewall** mag wijzigen
- **Bevestiging vragen voor** - specificeren aan wie de bevestigingsdialoogvensters (*dialoogvensters waarin een beslissing moet worden genomen in die gevallen die niet worden gedekt door een gedefinieerde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

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

- **Beheerder** – de beheerder heeft volledige controle over de pc en kan iedere gebruiker in groepen indelen met specifiek gedefinieerde rechten
- **Beheerder en hoofdgebruiker** – de beheerder kan iedere gebruiker in een specifieke groep (*Hoofdgebruiker*) indelen en rechten voor de groepsleden definiëren
- **Alle gebruikers** – andere gebruikers die niet aan een specifieke groep zijn toegewezen

10.3. Profielen van gebieden en adapters

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





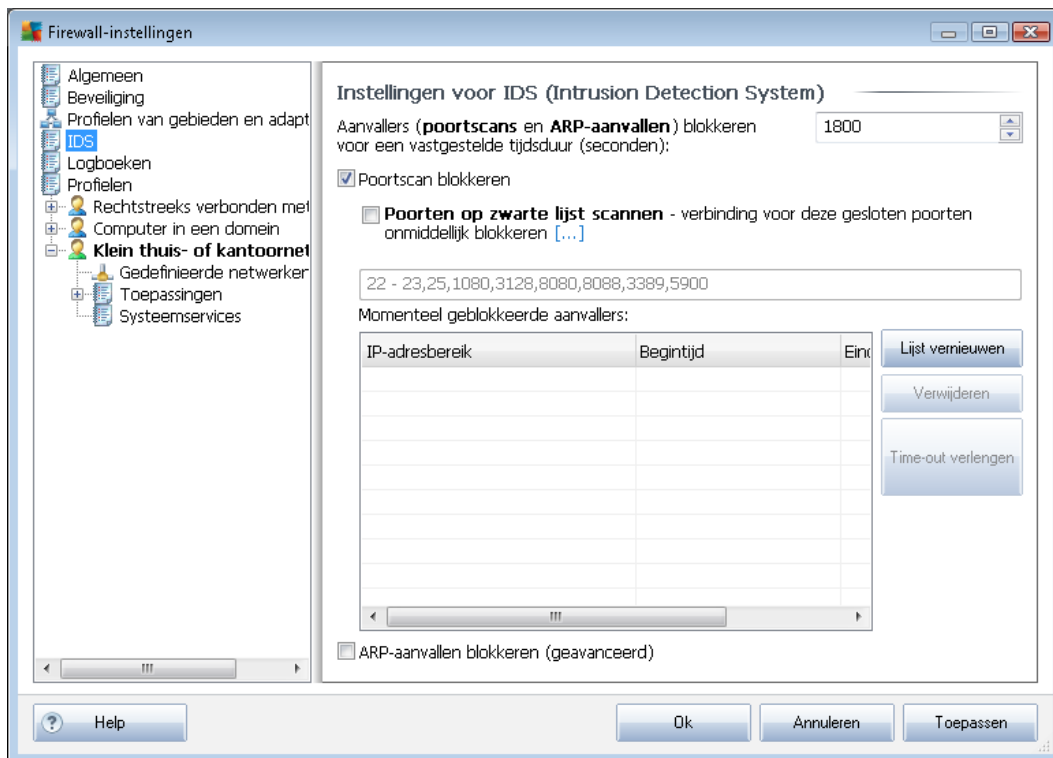
- **Gebieddetectie en automatische profielschakeling uitschakelen** – één van de gedefinieerde profielen kan worden toegewezen aan elk type netwerkinterface, respectievelijk aan elk gebied. Als u geen specifieke profielen wilt toewijzen, zal een algemeen profiel worden toegepast. Als u echter onderscheid wilt maken tussen profielen en ze wilt toewijzen aan specifieke adapters en gebieden en dan achteraf, om de één of andere reden, die ordening tijdelijk wilt wijzigen, schakelt u het selectievakje **Gebieddetectie en profielschakeling uitschakelen** in.
- **Lijst met gebieden en toegewezen profielen** – deze lijst biedt een overzicht van gedetecteerde adapters en gebieden. U kunt elk van hen een specifiek profiel toewijzen uit het menu met gedefinieerde profielen. Klik op een item in de lijst met adapters om het menu te openen en selecteer dan een profiel.

Geavanceerde instellingen

- **Altijd standaardprofiel gebruiken, dialoogvenster voor detectie van nieuw netwerk niet weergeven** – steeds wanneer de computer een verbinding tot stand brengt met een nieuw netwerk, wordt u door **Firewall** gewaarschuwd en wordt een dialoogvenster geopend, waarin u wordt gevraagd een type netwerkverbinding te kiezen en er een **Firewall-profiel** aan toe te kennen. Als u niet wilt dat het dialoogvenster wordt weergegeven, schakelt u dit selectievakje in.
- **Heuristische methode van AVG gebruiken voor detectie van nieuwe netwerken** – gegevens verzamelen over een nieuw gedetecteerd netwerk met het eigen mechanisme van AVG (*deze optie is alleen beschikbaar onder Windows Vista en hoger*).
- **Microsoft-methode gebruiken voor detectie van nieuwe netwerken** – informatie over nieuw ontdekte netwerken overnemen uit de Windows-service (*deze optie is alleen beschikbaar onder Windows Vista en hoger*).

10.4. IDS

Het **Intrusion Detection System** is een speciale gedragsherkenkende functie die is ontwikkeld om verdachte pogingen tot communicatie via bepaalde poorten van uw computer te herkennen en te blokkeren. U kunt in de volgende interface parameters instellen voor IDS:



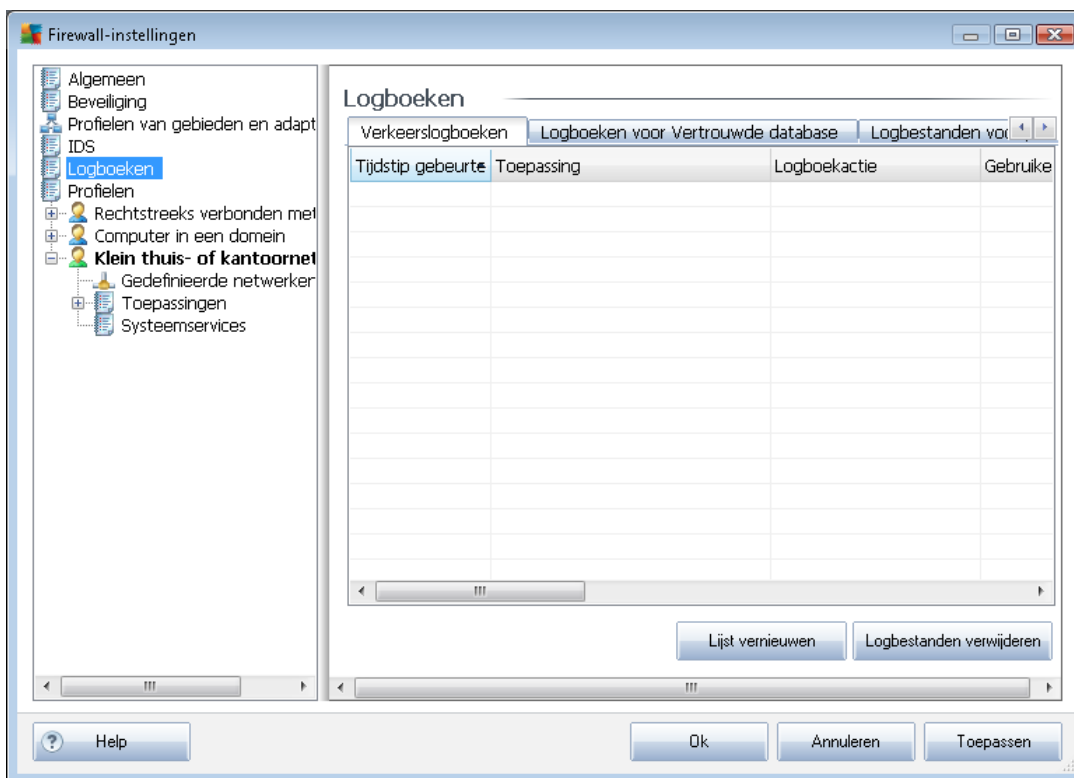
In het dialoogvenster **Intrusion Detection System (IDS)-instellingen** staan de volgende opties:

- **Aanvallers gedurende een bepaalde tijd blokkeren** – opgeven hoeveel seconden een poort geblokkeerd moet blijven als een verdachte poging tot communicatie via die poort wordt gedetecteerd. Standaard is de optie ingesteld op 1800 seconden (30 minuten).
- **Poortscan blokkeren** – alle pogingen tot communicatie met de computer van buitenaf via TCP- en UDP-poorten blokkeren. Bij elk van dergelijke verbindingen zijn vijf pogingen toegestaan, terwijl de zesde wordt geblokkeerd.
 - **Poortscan blokkeren** – direct alle pogingen tot communicatie via de in het eronder staande tekstvak opgegeven poorten blokkeren. Afzonderlijke poorten en poortreeksen moeten van elkaar worden gescheiden met komma's. Er is een vooraf opgestelde lijst met aanbevolen poorten voor deze optie, mocht u die willen gebruiken.
 - **Momenteel geblokkeerde aanvallers** – in dit gedeelte staan alle pogingen tot communicatie die op dit moment door de **firewall** worden tegengehouden. Een volledig overzicht van alle in het verleden geblokkeerde pogingen is te zien in het dialoogvenster **Logboeken**, op het tabblad **Poortscanlogboeken**.
- **ARP-aanvallen blokkeren** – een speciaal soort communicatiepogingen binnen een lokaal netwerk ('achter' de router), die door **IDS** als mogelijk gevaarlijk worden herkend, wordt geblokkeerd. Daarvoor geldt de tijdsduur die is ingesteld bij **Aanvallers gedurende een bepaalde tijd blokkeren**. We raden alleen ervaren gebruikers, die vertrouwd zijn met het type lokale netwerk en de risiconiveaus daarvan, aan gebruik te maken van deze functie.

Knoppen

- **Lijst vernieuwen** – de lijst bijwerken (*uitbreiden met de nieuwste geblokkeerde pogingen*)
- **Verwijderen** – een geselecteerde blokkade verwijderen
- **Time-out verlengen** – de tijd verlengen gedurende welke een geselecteerde poging is geblokkeerd. Er wordt dan een nieuw dialoogvenster geopend met opties voor het verlengen, waarin u een tijd en datum kunt opgeven, of een onbeperkte tijdsduur.

10.5. Logboeken



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

- **Verkeersmeldingen** – informatie over activiteiten van alle toepassingen die hebben geprobeerd verbinding te maken met het netwerk.
- **Meldingen Vertrouwde database** – de *Vertrouwde database* is de interne database van AVG waarin informatie wordt verzameld over gecertificeerde en vertrouwde toepassingen die altijd mag worden toegestaan online te communiceren. De eerste keer dat een nieuwe



toepassing probeert een verbinding tot stand te brengen met het netwerk (*terwijl er bijvoorbeeld nog geen firewallregel voor de toepassing is gedefinieerd*), moet worden uitgezocht of de desbetreffende toepassing mag communiceren via het netwerk. Eerst zoekt AVG in de *Vertrouwde database*, en als de toepassing daarin wordt vermeld, wordt automatisch toegang tot het netwerk verleend. Pas daarna, wanneer duidelijk is dat er geen informatie over de toepassing is opgeslagen in de *Vertrouwde database*, wordt u in een afzonderlijk dialoogvenster gevraagd of de toepassing toegang mag krijgen tot het netwerk.

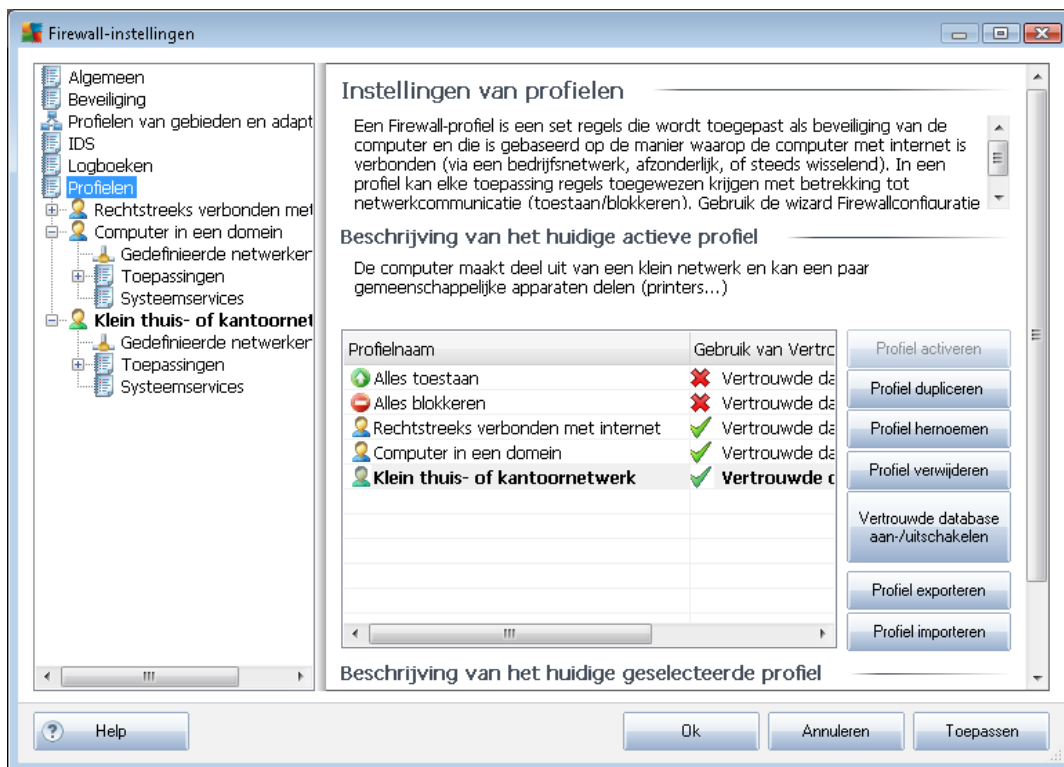
- **Logboek Poortscan** – registratie van alle activiteit van het [Intrusion Detection System](#) .
- **ARP-logboek** – registratie van informatie over het blokkeren van speciale soorten communicatiepogingen binnen een lokaal netwerk (optie [ARP-aanvallen blokkeren](#)) gedetecteerd door [Intrusion Detection System](#) als potentieel gevaarlijk.

Knoppen

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

10.6. Profielen

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



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

- **Profiel activeren** – met deze knop stelt u het geselecteerde profiel in als actief profiel, dat wil zeggen dat de geselecteerde profielconfiguratie zal worden gebruikt door de *firewall* bij het controleren van het netwerkverkeer
- **Profiel dupliceren** – er wordt een identieke kopie gemaakt van het geselecteerde profiel; vervolgens kunt u de kopie bewerken en een andere naam geven en zo een nieuw profiel maken gebaseerd op het geduplicateerde origineel.
- **Profiel hernoemen** – het geselecteerde profiel een nieuwe naam geven
- **Profiel verwijderen** – het geselecteerde profiel uit de lijst verwijderen
- **Vertrouwde database in-/uitschakelen** – u kunt opgeven of u voor het geselecteerde profiel de informatie uit de *Vertrouwde database* wilt gebruiken (*de Vertrouwde database is de interne database van AVG waarin informatie wordt verzameld over gecertificeerde en vertrouwde toepassingen die altijd mag worden toegestaan online te communiceren.*)
- **Profiel exporteren** – de configuratie van het geselecteerde profiel wordt opgeslagen in een bestand en kan in die vorm verder worden gebruikt



- **Profiel importeren** – de instellingen van het geselecteerde profiel worden geconfigureerd overeenkomstig de gegevens die worden opgehaald uit het back-upconfiguratiebestand

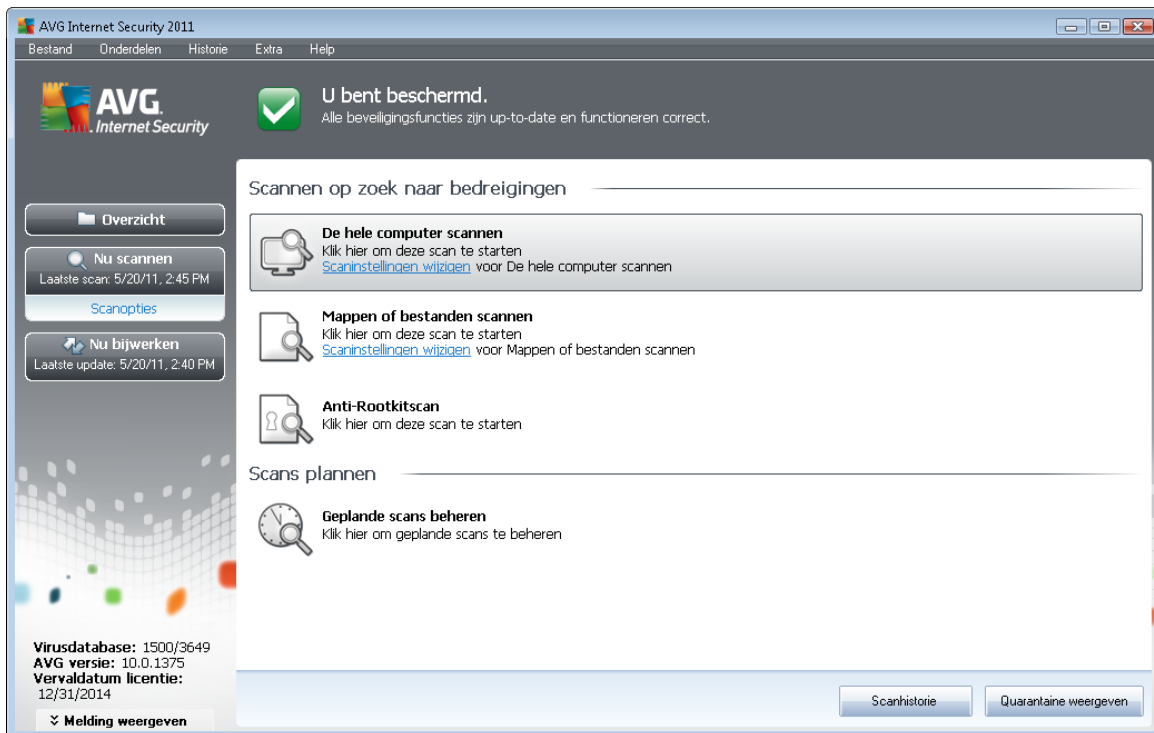
Onder in het dialoogvenster staat een beschrijving van het in de lijst erboven geselecteerde profiel.

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

11. AVG scannen

Scannen is een essentieel onderdeel van de functionaliteit van **AVG Internet Security 2011**. U kunt tests op verzoek uitvoeren of u kunt ze [plannen, zodat ze periodiek worden uitgevoerd](#) op tijdstippen waarop het u schikt

11.1. 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

11.2. Vooraf ingestelde scans

Een van de belangrijkste voorzieningen van **AVG Internet Security 2011** 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 uit te voeren. Dat geldt ook als u vermoedt dat er geen virussen op uw computer zullen worden gevonden.

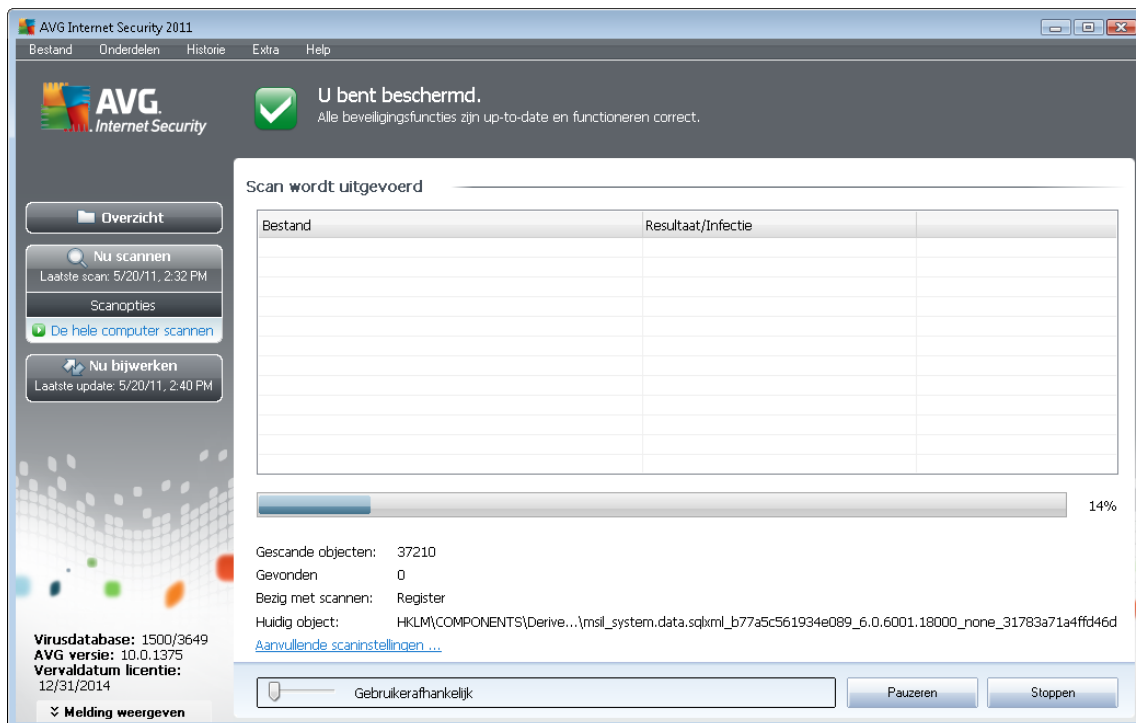
AVG Internet Security 2011 heeft twee scanmethodes die door de softwareleverancier van te voren zijn gedefinieerd:

11.2.1. 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.

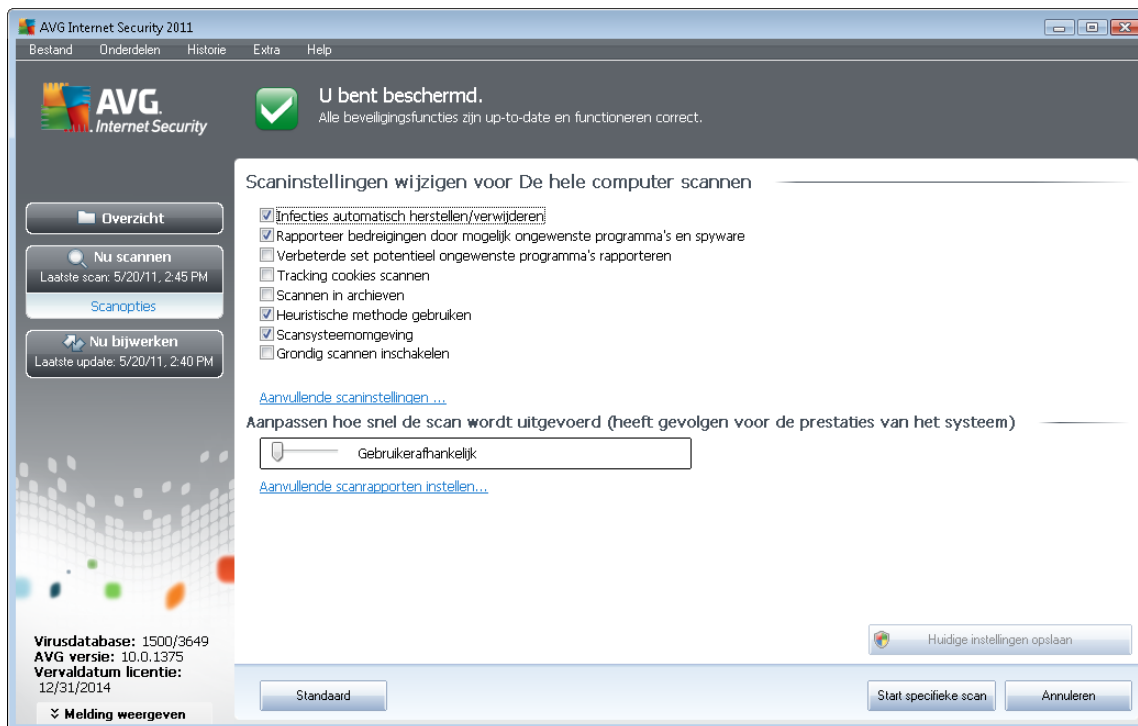
Scan starten

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

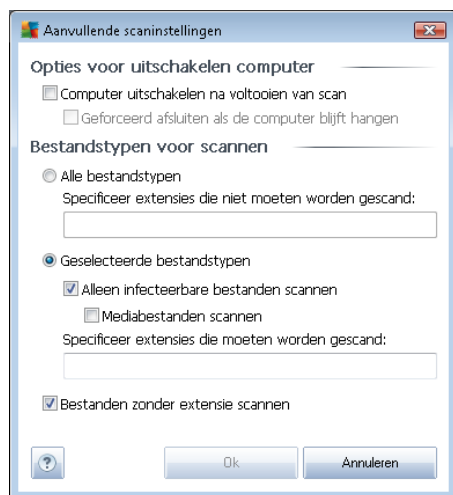
U kunt de vooraf gedefinieerde standaardinstellingen van **De hele computer scannen** wijzigen. Klik op de koppeling **Scaninstellingen wijzigen** om het dialoogvenster **Scaninstellingen wijzigen voor De hele computer scannen** (toegankelijk vanuit de [scaninterface](#) via de koppeling **Scaninstellingen 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 uitgeschakeld) – 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 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 voltooiën van scanproces**), wordt een tweede optie actief waarmee u de computer geforceerd kunt afsluiten, zelfs als die op dat moment is vergrendeld (**Geforceerd afsluiten als de computer vergrendeld is**).
- **Specificeer te scannen bestandstypen** – geef op wat u precies wilt scannen:
 - **Alle bestandstypen** – u kunt een lijst opgeven met door komma's gescheiden bestandsextensies die moeten worden genegeerd bij het scannen;

- **Geselecteerde bestandstypen** – u kunt opgeven dat u alleen bestanden wilt scannen die mogelijk geïnfecteerd kunnen worden (*bestanden die niet geïnfecteerd kunnen worden, worden niet gescand, bijvoorbeeld bepaalde niet-opgemaakte tekstbestanden, of andere bestanden die niet uitvoerbaar zijn*), inclusief mediabestanden (*videobestanden, audiobestanden – als u deze optie niet inschakelt, reduceert u de tijd die nodig is voor het scannen nog meer, omdat dit vaak grote bestanden zijn met een kleine kans op virusinfecties*). U kunt ook nu aan de hand van extensies opgeven welke bestanden altijd moeten worden gescand.
- U kunt bovendien aangeven of u **bestanden zonder extensie wilt scannen** – deze optie is standaard ingeschakeld en we raden u aan deze instelling aan te houden, tenzij u een goede reden hebt om die te wijzigen. Bestanden zonder extensie zijn uitermate verdacht en dienen altijd te worden gescand.
- **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.

11.2.2. 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.

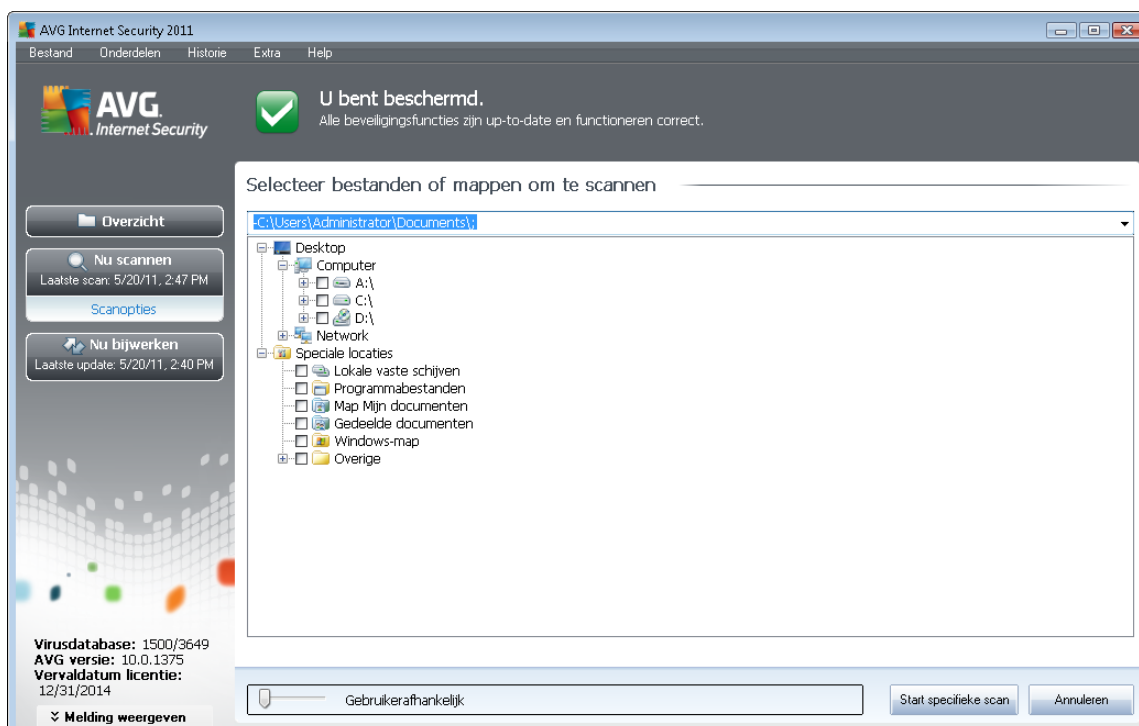


Scan starten

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.

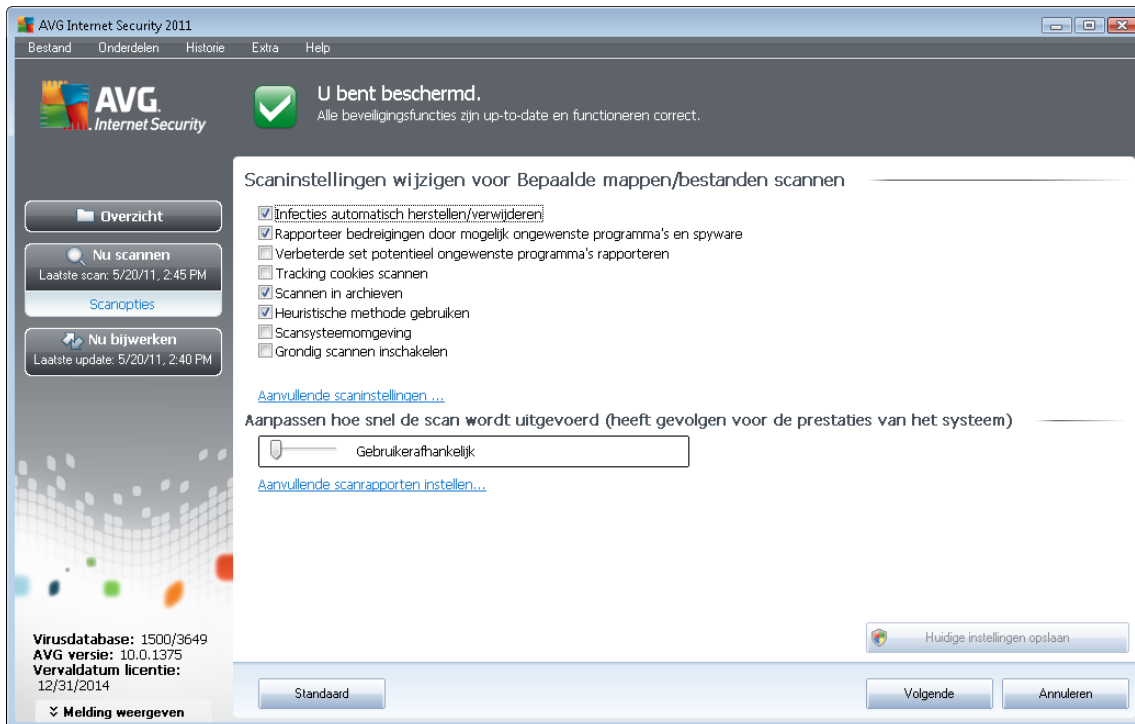
U kunt ook een map scannen, maar tegelijkertijd alle submappen van die map uitsluiten van het scannen; daartoe typt u een minteken "-" voor het automatisch gegenereerde pad (zie de [schermafbeelding](#)). Als u de hele map wilt uitsluiten van het scannen, gebruikt u de "!"- parameter.

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

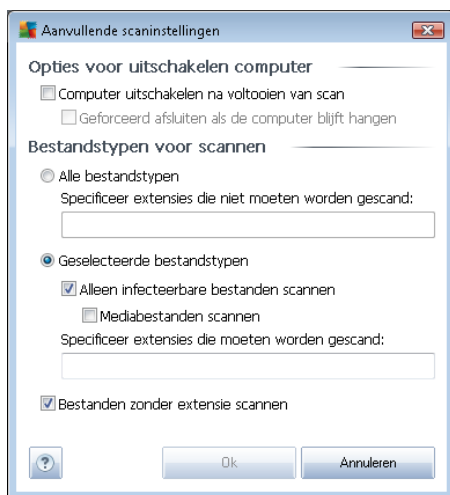
U kunt de vooraf gedefinieerde standaardinstellingen van **Bepaalde mappen of bestanden scannen** wijzigen. Klik op de koppeling **Scaninstellingen wijzigen** om het dialoogvenster **Scaninstellingen wijzigen voor Bepaalde mappen of bestanden scannen** te openen. **Het is raadzaam de standaardinstellingen 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 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 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 voltooiën van scanproces**), wordt een tweede optie actief waarmee u de computer geforceerd kunt afsluiten, zelfs als die op dat moment is vergrendeld (**Geforceerd afsluiten als de computer vergrendeld is**).
- **Specificeer te scannen bestandstypen** – geef op wat u precies wilt scannen:
 - **Alle bestandstypen** – u kunt een lijst opgeven met door komma's gescheiden bestandsextensies die moeten worden genegeerd bij het scannen;

- **Geselecteerde bestandstypen** – u kunt opgeven dat u alleen bestanden wilt scannen die mogelijk geïnfecteerd kunnen worden (*bestanden die niet geïnfecteerd kunnen worden, worden niet gescand, bijvoorbeeld bepaalde niet-opgemaakte tekstbestanden, of andere bestanden die niet uitvoerbaar zijn*), inclusief mediabestanden (*videobestanden, audiobestanden – als u deze optie niet inschakelt, reduceert u de tijd die nodig is voor het scannen nog meer, omdat dit vaak grote bestanden zijn met een kleine kans op virusinfecties*). U kunt ook nu aan de hand van extensies opgeven welke bestanden altijd moeten worden gescand.
- U kunt bovendien aangeven of u **bestanden zonder extensie wilt scannen** – deze optie is standaard ingeschakeld en we raden u aan deze instelling aan te houden, tenzij u een goede reden hebt om die te wijzigen. Bestanden zonder extensie zijn uitermate verdacht en dienen altijd te worden gescand.
- **Prioriteit scanproces** – met de schuifbalk kunt u de prioriteit voor het scanproces wijzigen. Standaard is 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](#)).

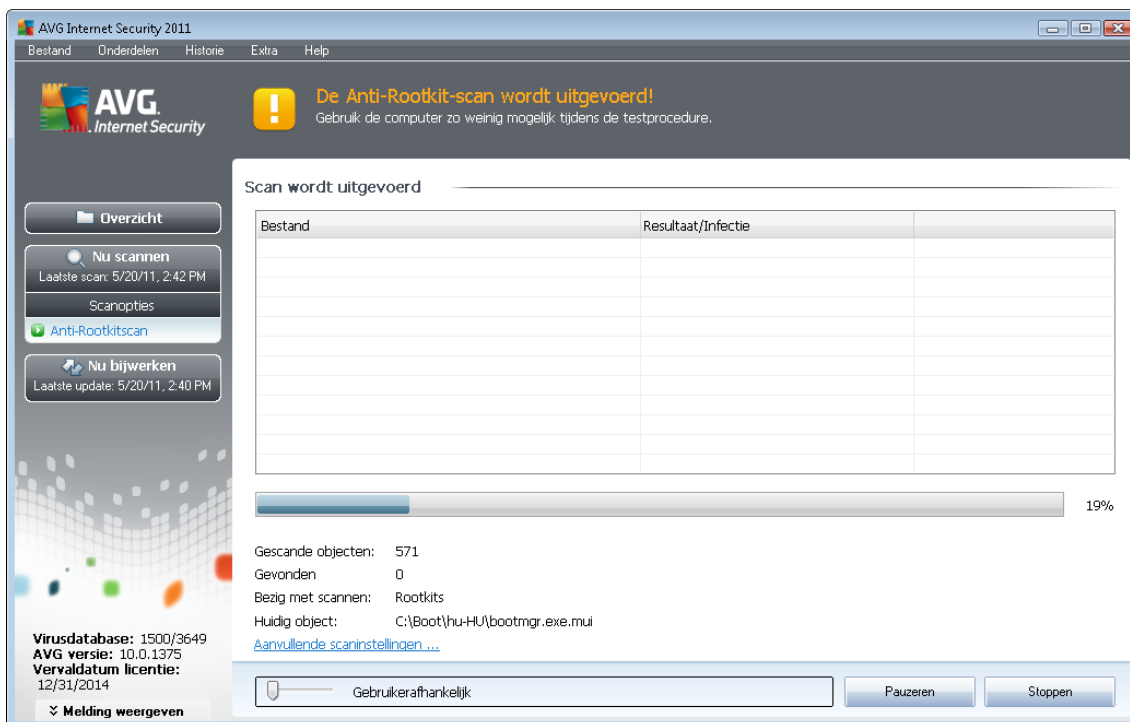
11.2.3. Antirootkitscan

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.

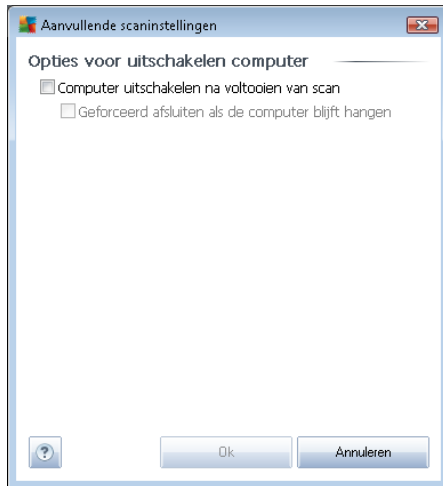


Scanconfiguratie bewerken

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:

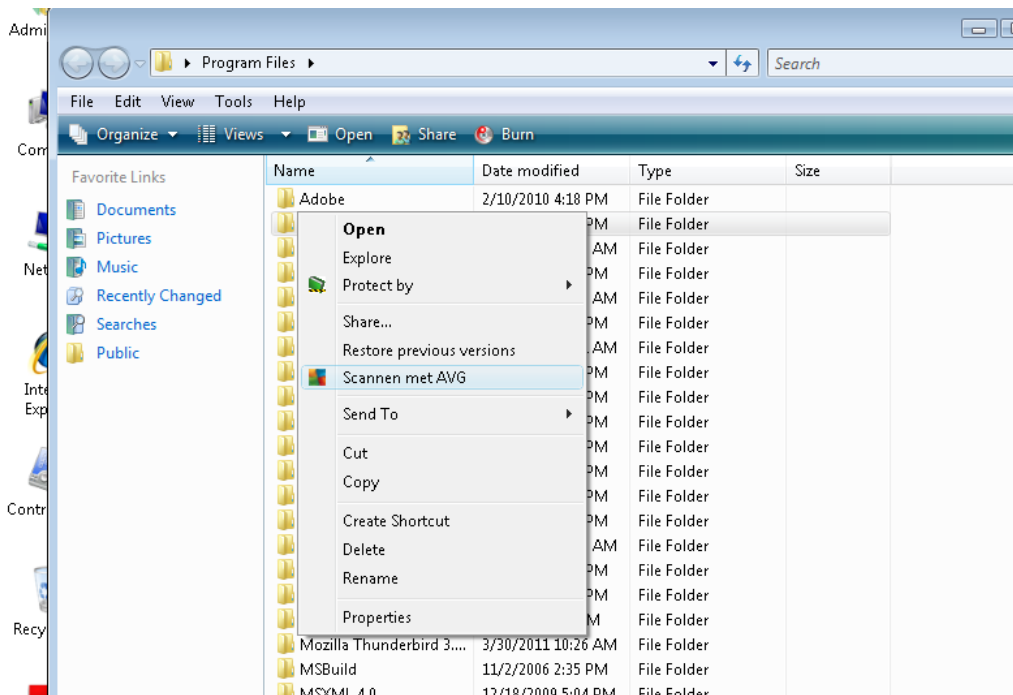
- **Automatische scan** – met de schuifbalk kunt u de prioriteit voor het scanproces wijzigen. Standaard is deze functie ingesteld op het niveau *gebruikerafhankelijk* voor gebruik van systeembronnen. U kunt ook langzamer scannen, wat betekent dat een minder groot beroep wordt gedaan op systeembronnen (*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**):



11.3. 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 Internet Security 2011** ook snel een specifiek object scannen in Windows Verkenner. Als u een onbekend bestand wilt openen en niet zeker weet of de inhoud veilig is, kunt u het op verzoek scannen. Ga als volgt te werk:



- Selecteer in Windows Verkenner het bestand (of de map) die u wilt controleren
- Klik met de rechtermuisknop op het object om het snelmenu te openen



- Kies de optie **Scannen met AVG** om het bestand te scannen met AVG

11.4. Scannen vanaf opdrachtregel

In **AVG Internet Security 2011** hebt u de mogelijkheid om een scan uit te voeren vanaf de opdrachtregel. Die optie kunt u bijvoorbeeld op servers gebruiken, of voor het maken van een batch-script dat onmiddellijk na het opstarten van de computer moet worden uitgevoerd. U kunt vanaf de opdrachtregel scans starten met vrijwel alle parameters die beschikbaar zijn in de grafische gebruikersinterface van AVG.

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

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

Syntaxis van de opdracht

De opdracht volgt de onderstaande syntaxis:

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

Scanparameters

Als u een volledig overzicht wilt weergeven van beschikbare parameters, typt u de betreffende opdracht samen met de parameter **/?** of **/HELP** (bijv. **avgscanx /?**). De enige verplichte parameter is **/SCAN** om te specificeren welke gedeeltes 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.

11.4.1. 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=path;path (e.g. /SCAN=C:\;D:\)
- **/COMP** [De hele computer scannen](#)
- **/HEUR** [Heuristische analyse](#) gebruiken
- **/EXCLUDE** Pad of bestanden uitsluiten van scan
- **/@** Opdrachtbestand /bestandsnaam/
- **/EXT** Deze extensies scannen /bijvoorbeeld EXT=EXE,DLL/
- **/NOEXT** Deze extensies niet scannen /bijvoorbeeld NOEXT=JPG/
- **/ARC** Archieven scannen
- **/CLEAN** Automatisch opschonen
- **/TRASH** Geïnfekteerde 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 geïnfekteerde bestanden als OK in rapport opnemen
- **/NOBREAK** CTRL-BREAK niet toestaan voor afbreken
- **/BOOT** MBR/BOOT-controle inschakelen
- **/PROC** Scannen actieve processen
- **/PUP** "[Potentieel ongewenste programma's](#)" in rapport opnemen



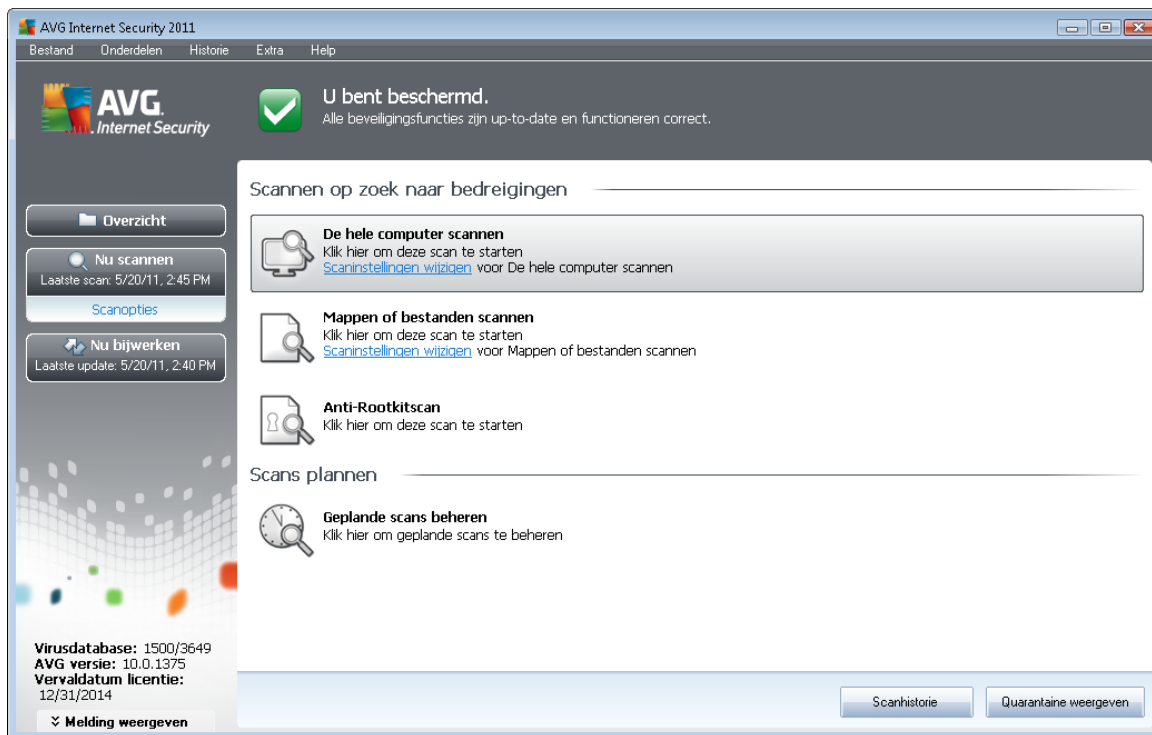
- **/REG** Register scannen
- **/COO** Cookies scannen
- **/?** Help over dit onderwerp weergeven
- **/HELP** Help over dit onderwerp weergeven
- **/PRIORITY** Stel de scanprioriteit in op /Langzaam, Auto, Snel/ (zie [Geavanceerde instellingen / Scans](#))
- **/SHUTDOWN** Computer uitschakelen na voltooiën van scan
- **/FORCESHUTDOWN** Computer geforceerd uitschakelen na voltooiën van scan
- **/ADS** Alternatieve gegevensstromen scannen (alleen NTFS)
- **/ARCBOMBSW** Meervoudig gecomprimeerde bestanden opnemen in rapport

11.5. Scans plannen

Met **AVG Internet Security 2011** kunt u scans op verzoek uitvoeren (bijvoorbeeld als u vermoedt dat uw computer geïnfecteerd is geraakt) of volgens schema. Het is met nadruk raadzaam om de scans op basis van een schema uit te voeren: op die manier weet u zeker dat uw computer wordt beschermd tegen alle mogelijke infecties, en hoeft u zich geen zorgen te maken over de vraag of en wanneer u een scan moet uitvoeren.

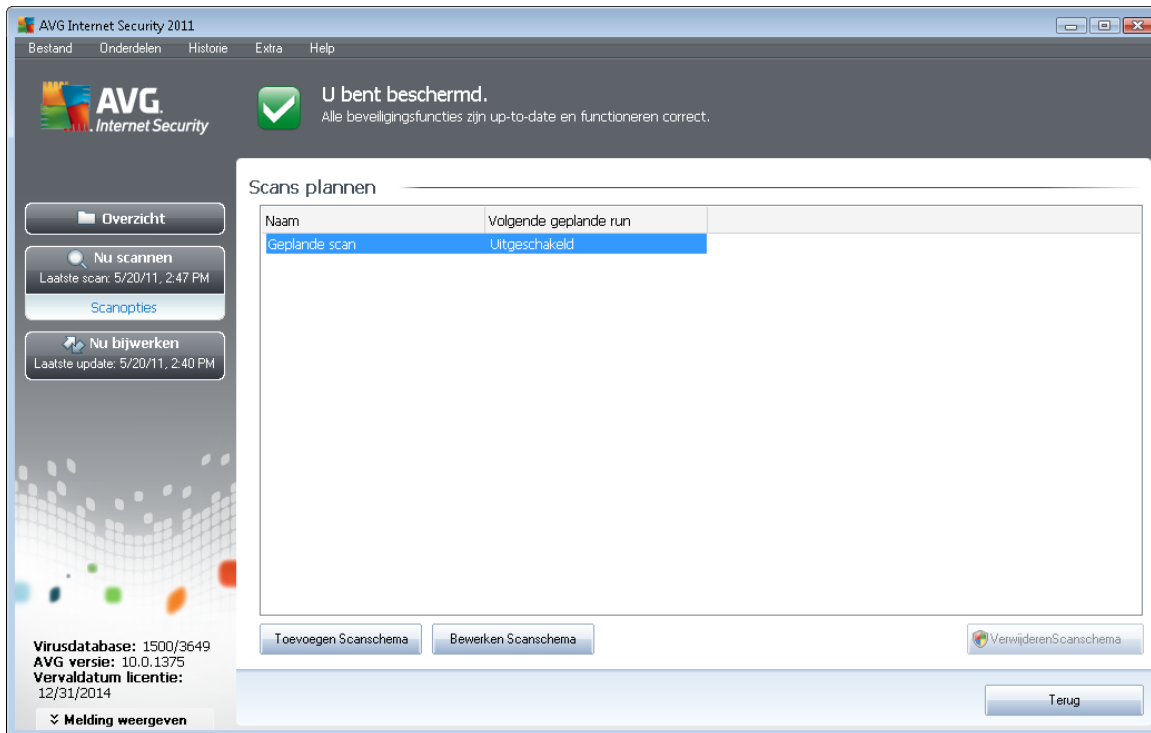
Minimaal voert u [De hele computer scannen](#) regelmatig uit, minstens één maal per week. Als het echter mogelijk is, is het verstandig om de hele computer dagelijks te scannen – zoals ook is ingesteld in de standaardconfiguratie voor scanschema's. Als de computer altijd "aan staat", kunt u de scans buiten kantooruren plannen. Als de computer zo nu en dan wordt uitgeschakeld, kunt u plannen dat scans [worden uitgevoerd bij het opstarten van de computer, als er een scan is overgeslagen](#).

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



Scans plannen

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

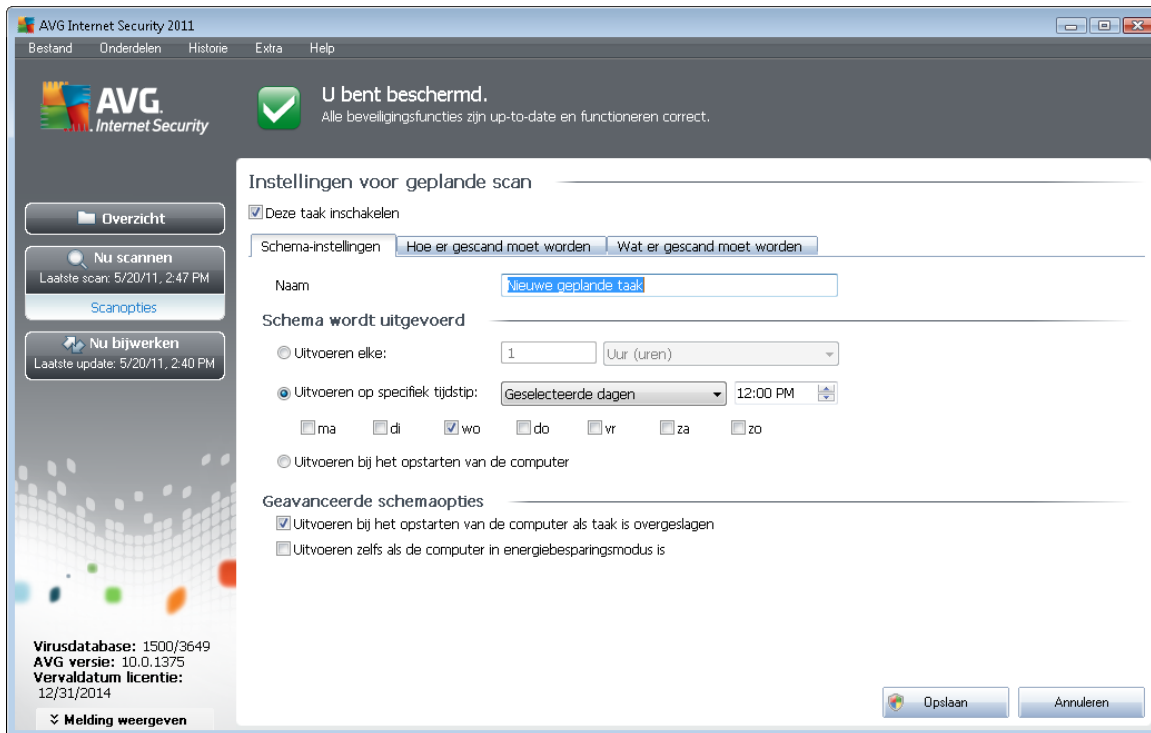


U kunt scans bewerken/toevoegen met de volgende knoppen:

- **Scanschema toevoegen** – als u op deze knop klikt, wordt het dialoogvenster **Instellingen voor geplande scan** geopend met het tabblad **Schema-instellingen**. In dat dialoogvenster kunt u de instellingen opgeven voor de nieuwe scan.
- **Scanschema bewerken** – deze knop is alleen actief als u eerst een bestaande scan uit de lijst met geplande scans hebt geselecteerd. In dat geval wordt de knop actief en kunt u erop klikken om het dialoogvenster **Instellingen voor geplande scan** te openen, met het tabblad **Schema-instellingen**. De parameters van de bestaande scan worden weergegeven, u kunt die wijzigen.
- **Scanschema verwijderen** – deze knop is eveneens alleen actief als u eerst een bestaande scan uit de lijst met geplande scans hebt geselecteerd. U kunt dat schema dan verwijderen als u op deze knop klikt. U kunt echter alleen uw eigen schema's verwijderen; het vooraf gedefinieerde **Schema volledige computer scannen** van de standaardinstellingen kan nooit worden verwijderd.
- **Terug** – terugkeren naar de [scaninterface van AVG](#)

11.5.1. Schema-instellingen

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



Op het tabblad **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



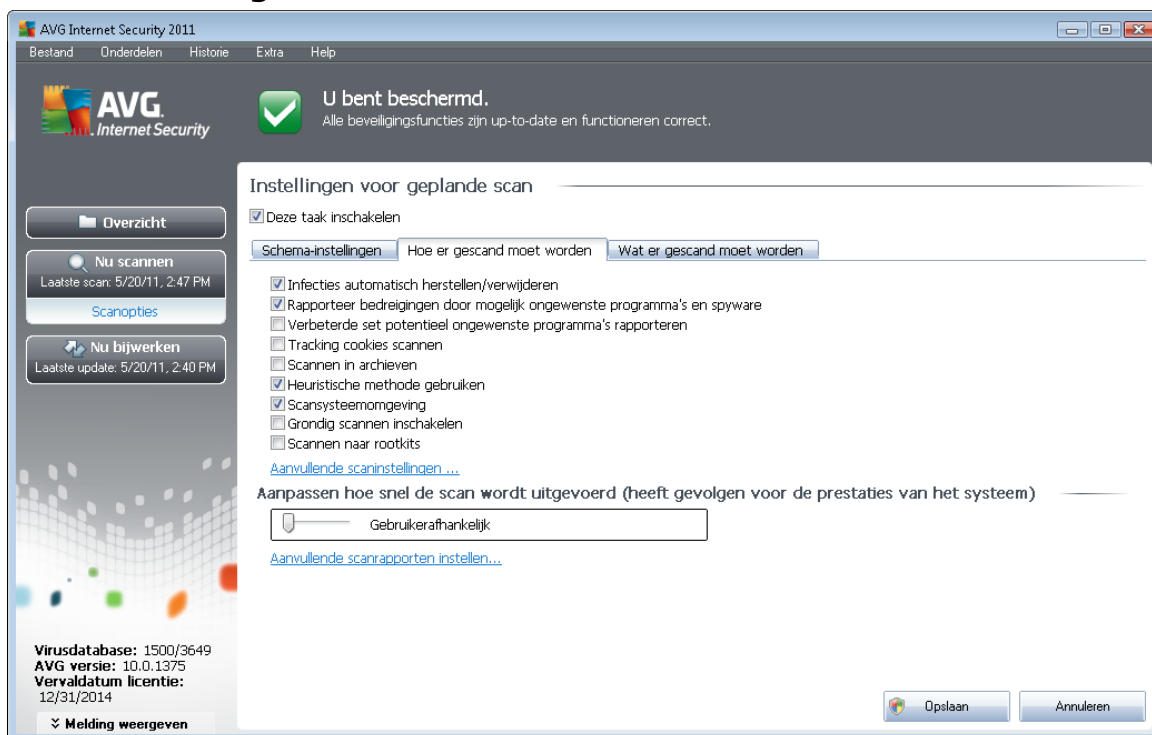
energiebesparingsmodus is of helemaal is uitgeschakeld.

Knoppen in het dialoogvenster Instellingen voor scanschema

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

- **Opslaan** – opslaan van alle wijzigingen die u hebt aangebracht 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](#).

11.5.2. Hoe er gescand moet worden



Op het tabblad **Hoe er gescand moet worden** staat een lijst met scanparameters die kunnen worden in- en uitgeschakeld. Standaard zijn de meeste parameters ingeschakeld en wordt de desbetreffende functionaliteit gebruikt bij het scannen. We raden u aan deze vooraf ingestelde configuratie aan te houden, tenzij u een goede reden hebt om deze instellingen te wijzigen:

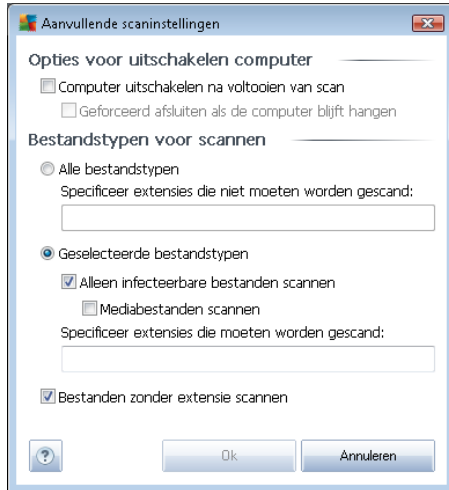
- **Infecties automatisch herstellen/verwijderen** (standaard ingeschakeld) – als tijdens het

scannen een virus wordt gedetecteerd, wordt automatisch een herstelprocedure gestart, als die beschikbaar is. Als het geïnfecteerde bestand niet automatisch hersteld kan worden, of als u besluit deze optie uit te schakelen, wordt u bij detectie van een virus gewaarschuwd en zult u op dat moment moeten besluiten wat u wilt doen met de gedetecteerde infectie. Het is raadzaam het geïnfecteerde bestand te verplaatsen naar de [Quarantaine](#).

- **Bedreigingen door mogelijk ongewenste programma's en spyware rapporteren** (standaard ingeschakeld) – schakel dit selectievakje in om de [Anti-Spyware](#)-engine te activeren en naar spyware en virussen te scannen. [Spyware behoort tot een twijfelachtige categorie malware: 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 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.

U kunt de scanconfiguratie als volgt wijzigen:

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



- o **Opties voor uitschakelen computer** – opgeven of de computer automatisch moet worden uitgeschakeld als het scanproces is voltooid. Als u die optie bevestigt (**Computer afsluiten na voltooi van scanproces**), wordt een tweede optie actief waarmee u de computer geforceerd kunt afsluiten, zelfs als die op dat moment is vergrendeld (**Geforceerd afsluiten als de computer vergrendeld is**).
- o **Specificeer te scannen bestandstypen** – geef op wat u precies wilt scannen:
 - **Alle bestandstypen** – u kunt een lijst opgeven met door komma's gescheiden bestandsextensies die moeten worden genegeerd bij het scannen;
 - **Geselecteerde bestandstypen** – u kunt opgeven dat u alleen bestanden wilt scannen die mogelijk geïnfecteerd kunnen worden (*bestanden die niet geïnfecteerd kunnen worden, worden niet gescand, bijvoorbeeld bepaalde niet-opgemaakte tekstbestanden, of andere bestanden die niet uitvoerbaar zijn*), inclusief mediabestanden (*videobestanden, audiobestanden – als u deze optie niet inschakelt, reduceert u de tijd die nodig is voor het scannen nog meer, omdat dit vaak grote bestanden zijn met een kleine kans op virusinfecties*). U kunt ook nu aan de hand van extensies opgeven welke bestanden altijd moeten worden gescand.
 - U kunt bovendien aangeven of u **bestanden zonder extensie wilt scannen** – deze optie is standaard ingeschakeld en we raden u aan deze instelling aan te houden, tenzij u een goede reden hebt om die te wijzigen. Bestanden zonder extensie zijn uitermate verdacht en dienen altijd te worden gescand.
- **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

dialogoogvenster geopend, **Scanrapporten**, waarin u kunt aangeven wat voor soort resultaten moeten worden gerapporteerd:



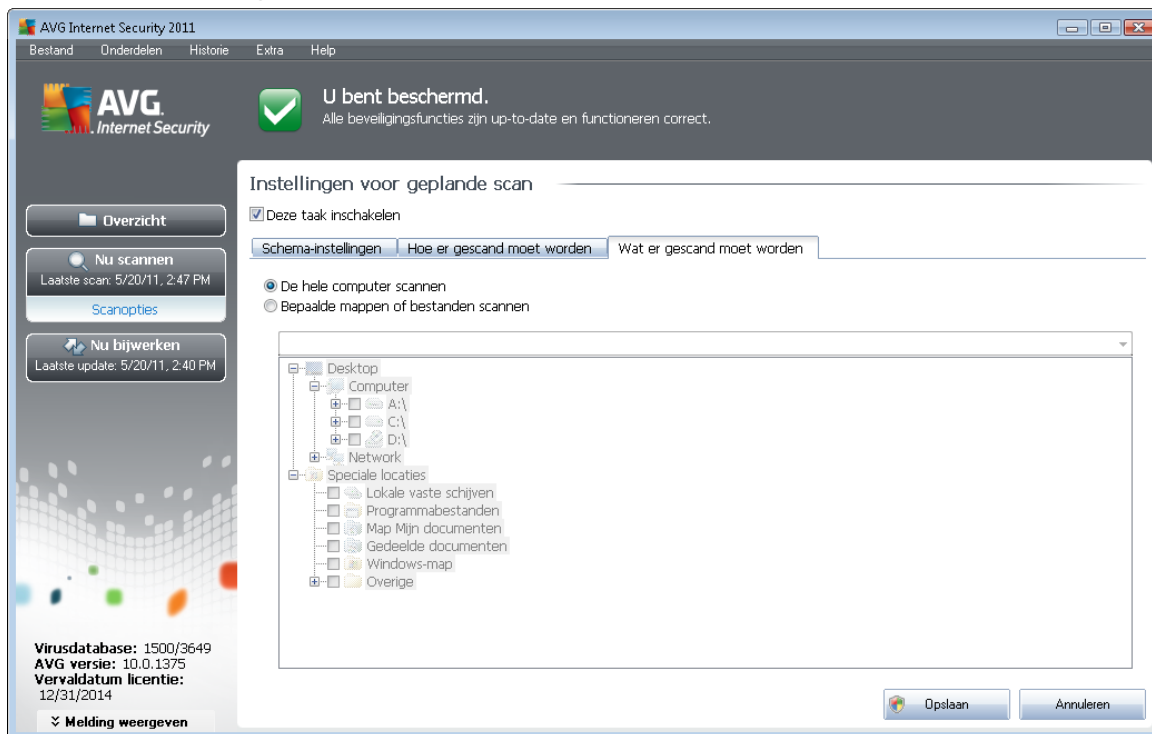
Opmerking: standaard is de scanconfiguratie ingesteld op optimale prestaties. Het is raadzaam de vooraf ingestelde configuratie aan te houden, tenzij u een goede reden hebt om de scaninstellingen te wijzigen. Alleen ervaren gebruikers dienen wijzigingen aan te brengen in de configuratie. Zie het dialoogvenster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

Knoppen

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

- **Opslaan** – opslaan van alle wijzigingen die u hebt uitgevoerd op dit tabblad of een van de twee andere tabbladen van het dialoogvenster, het dialoogvenster sluiten en terugkeren naar het [standaarddialoogvenster van de AVG scaninterface](#). Klik daarom, als u 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](#).

11.5.3. 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**



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

- **Gedeelde documenten**

- o voor Win XP: C:\Documents and Settings\All Users\Documents\
- o voor Windows Vista/7: C:\Users\Public\Documents\

- **Map Windows** – C:\Windows\

- **Overig**

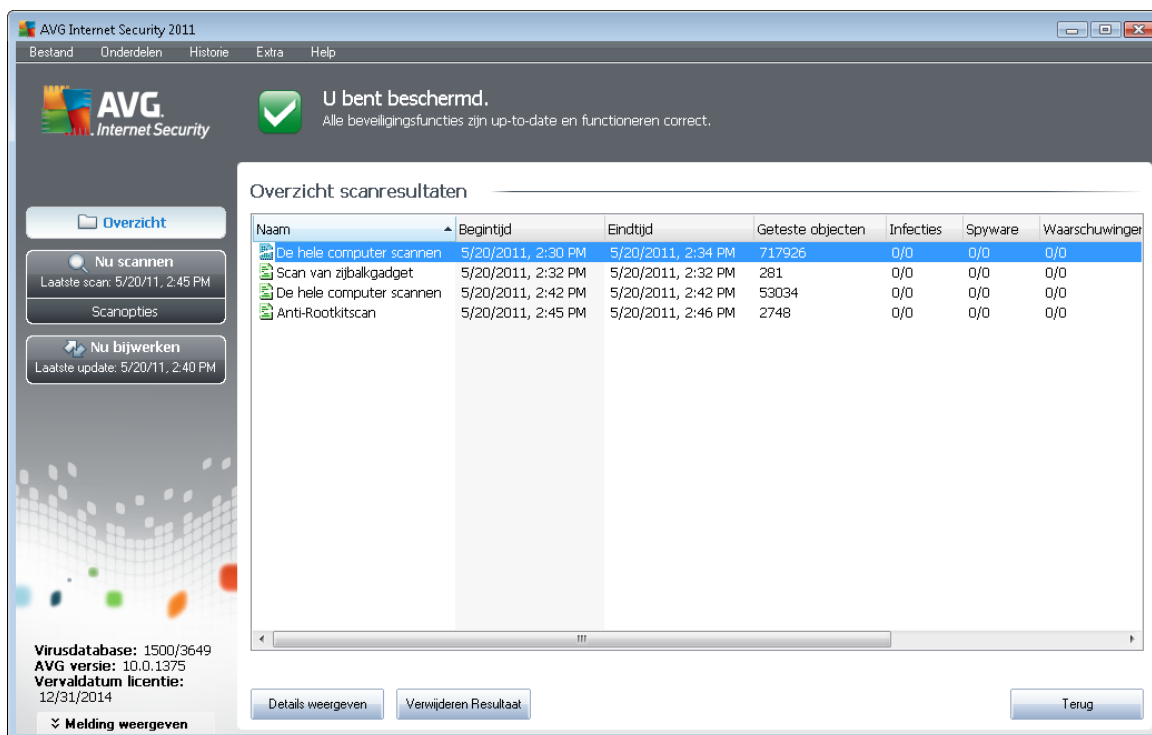
- o **Systeemstation** – de vaste schijf waarop het besturingssysteem is geïnstalleerd (meestal C:)
- o **Systeemmap** – Windows/System32\
- o **Map tijdelijke bestanden** – C:\Documents and Settings\User\Local\ (Windows XP) of C:\Users\user\AppData\Local\Temp\ (Windows Vista/7)
- o **Tijdelijke internetbestanden** – 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 in het dialoogvenster Instellingen voor scanschema

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


- **Opslaan** – opslaan van alle wijzigingen die u hebt aangebracht 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](#).


11.6. Overzicht scanresultaten




U kunt het dialoogvenster **Overzicht scanresultaten** openen als u in de [AVG scaninterface](#) op de knop **Scanhistoriek** 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 voltooiën 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](#)

11.7. Details scanresultaten

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

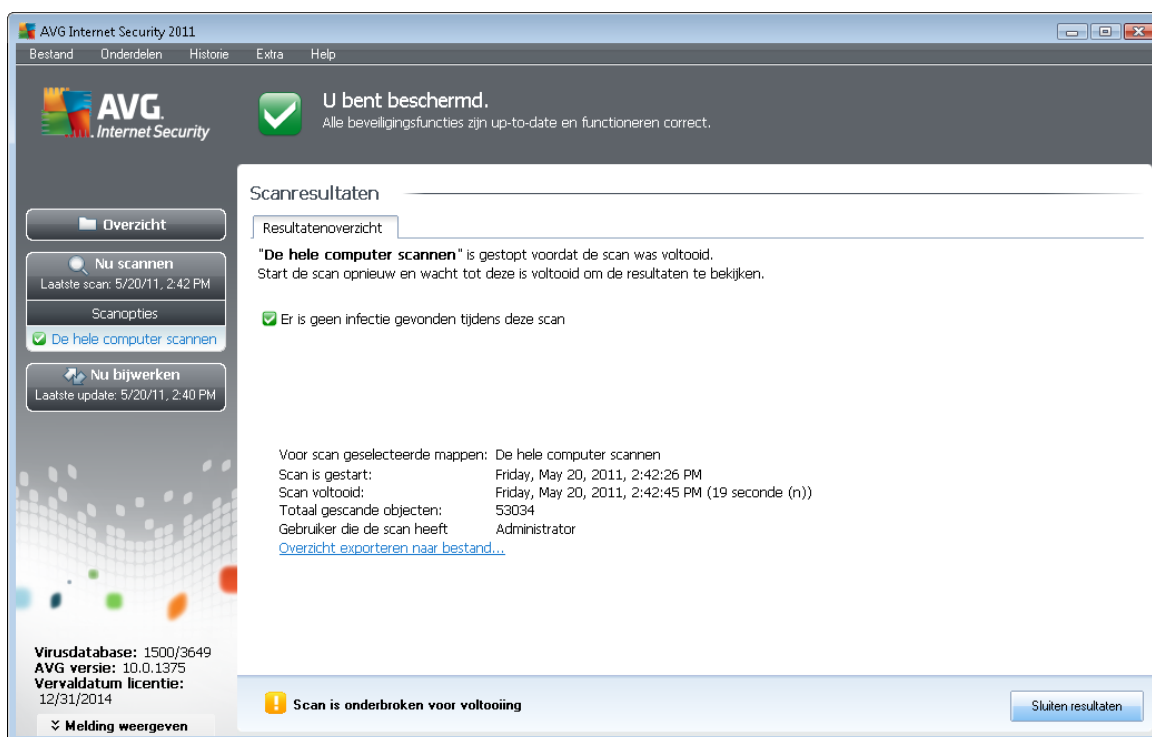
Het dialoogvenster heeft bovendien een aantal tabbladen:

- [Resultatenoverzicht](#) - dit tabblad wordt steeds weergegeven en bevat statistische gegevens over de voortgang van het scanproces
- [Infecties](#) - dit tabblad wordt alleen weergegeven als een [virusinfectie](#) is gedetecteerd tijdens het scannen
- [Spyware](#) - dit tabblad wordt alleen weergegeven als [spyware](#) is gedetecteerd tijdens het scannen
- [Waarschuwingen](#) - deze tab wordt bijvoorbeeld weergegeven als er cookies zijn gedetecteerd tijdens het scannen
- [Rootkits](#) - dit tabblad wordt alleen weergegeven als er [rootkits](#) zijn gedetecteerd tijdens het

scannen

- **Informatie** - dit tabblad wordt alleen weergegeven als er potentiële gevaren zijn gedetecteerd die niet in de bovenstaande categorieën kunnen worden ondergebracht; in dat geval staat er op het tabblad een waarschuwing met betrekking tot de vondst. U vindt hier ook informatie over objecten die niet konden worden gescand (bijvoorbeeld archieven die met een wachtwoord zijn beveiligd).

11.7.1. Tabblad Overzicht resultaten



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

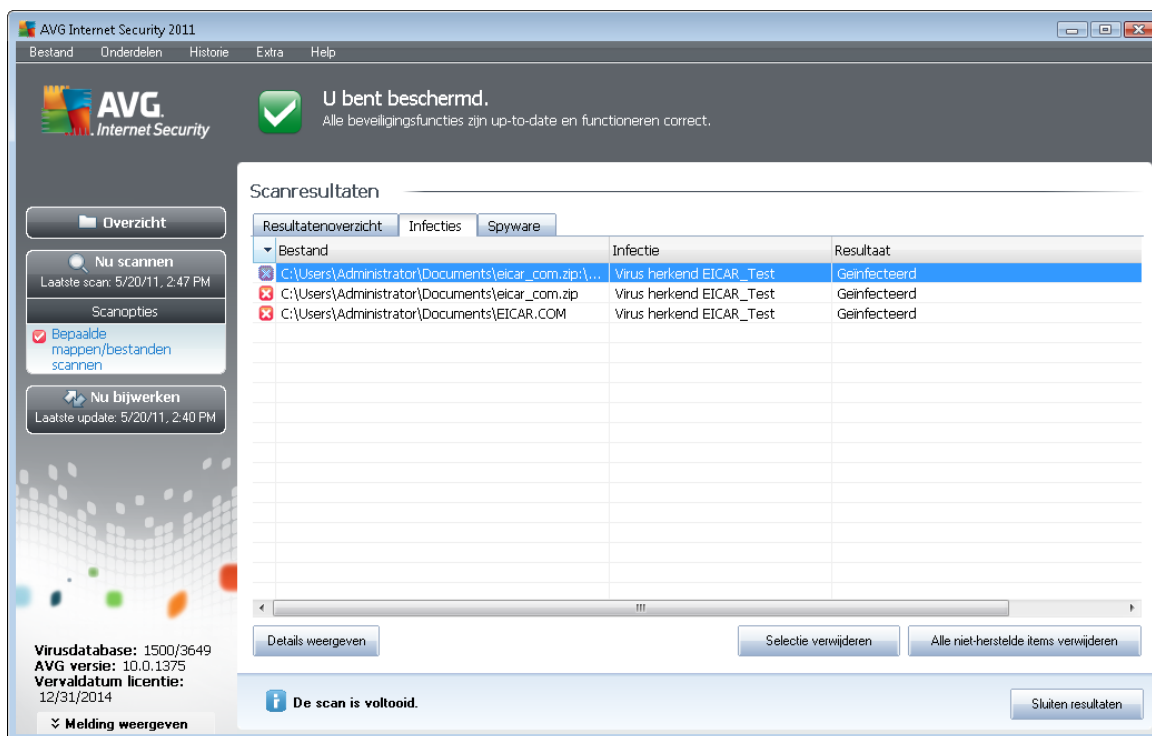
- gedetecteerde [virusinfecties](#) / [spyware](#)
- verwijderde [virusinfecties](#) / [spyware](#)
- de hoeveelheid [virusinfecties](#) / [spyware](#) die niet kan worden verwijderd of hersteld

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

Knoppen

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

11.7.2. 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

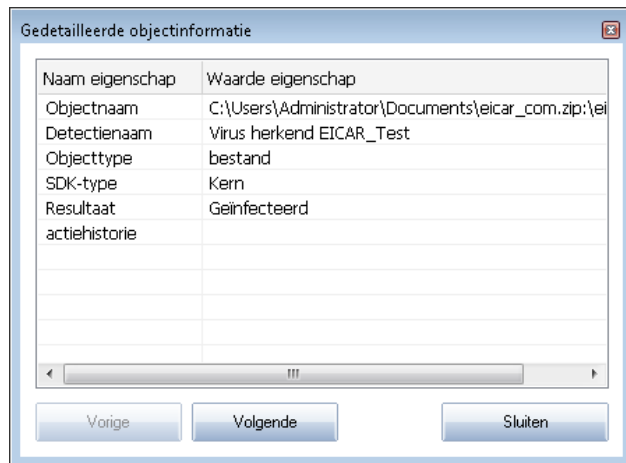
object tot de uitzonderingen behoort en het object is toegevoegd aan de lijst met PUP-uitzonderingen (*geconfigureerd bij [PUP-uitzonderingen](#) in het dialoogvenster Geavanceerde instellingen*)

- **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:

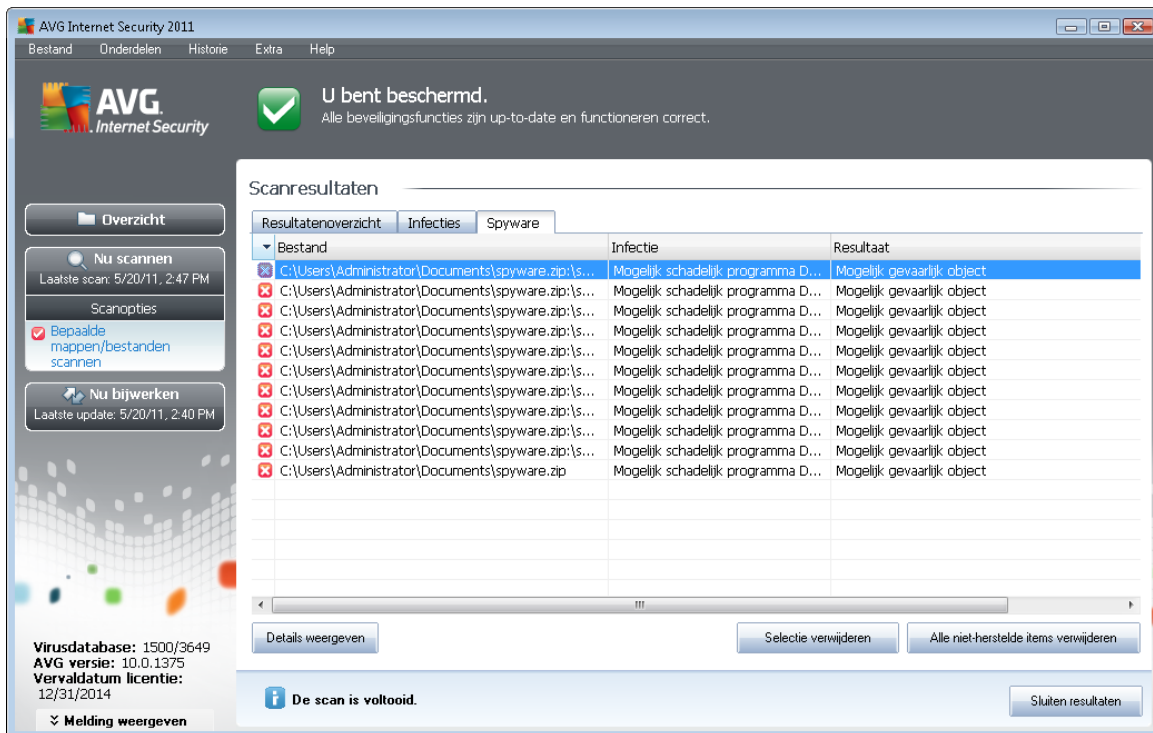


In dit dialoogvenster staat gedetailleerde informatie over het gedetecteerde geïnfecteerde object (*bijv. naam, locatie, type van het object, SDK-type, detectieresultaat en actiehistorie met betrekking tot het gedetecteerde object*). Gebruik de knoppen **Vorige** / **Volgende** om informatie te bekijken 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](#)

11.7.3. Tabblad Spyware



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

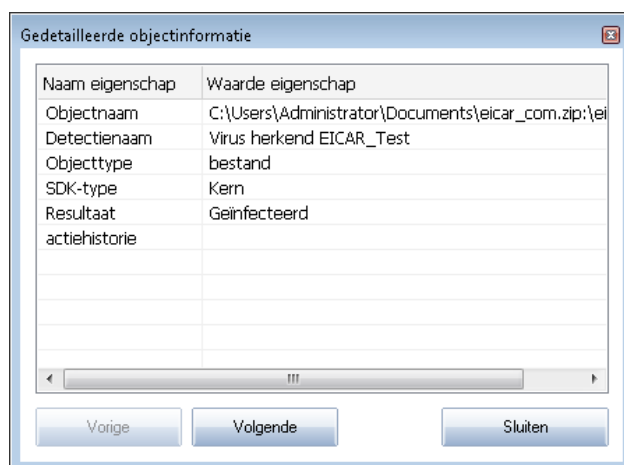
- **Bestand** – het volledige pad naar de oorspronkelijke locatie van het geïnfecteerde object
- **Infecties** – de naam van de gedetecteerde [spyware](#) (*raadpleeg de online [Virusencyclopedie](#) voor meer informatie over specifieke virussen*)
- **Resultaat** – de huidige status van het object dat tijdens het scannen is gedetecteerd:
 - **Geïnfecteerd** – het geïnfecteerde object is gedetecteerd, maar niet van de oorspronkelijke locatie verwijderd (bijvoorbeeld omdat u [de functie voor automatisch herstel hebt uitgeschakeld](#) bij bepaalde scaninstellingen)
 - **Hersteld** – het geïnfecteerde object is automatisch hersteld en niet van de oorspronkelijke locatie verwijderd
 - **Verplaatst naar de Quarantaine** – het geïnfecteerde object is verplaatst naar de [Quarantaine](#)
 - **Verwijderd** – het geïnfecteerde object is verwijderd

- **Toegevoegd aan de PUP-uitzonderingen** – er is vastgesteld dat het gevonden object tot de uitzonderingen behoort en het object is toegevoegd aan de lijst met PUP-uitzonderingen (geconfigureerd bij [PUP-uitzonderingen](#) in het dialoogvenster Geavanceerde instellingen)
- **Vergrendeld bestand – niet 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](#)

11.7.4. Tabblad Waarschuwingen

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

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

- **Verborgen bestanden** - de verborgen bestanden zijn standaard niet zichtbaar in Windows, en sommige virussen of andere bedreigingen kunnen detectie proberen te vermijden door hun bestanden op te slaan met dit kenmerk. Als AVG een verborgen bestand rapporteert dat u verdacht of kwaadaardig voorkomt, kunt u het verplaatsen naar de [AVG Quarantaine](#).
- **Cookies** - cookies zijn tekstbestanden die worden gebruikt door websites voor het opslaan van gebruikersspecifieke informatie, die later wordt gebruikt voor het laden van aangepaste websitelayouts, het vooraf invullen van gebruikersnamen, etc.
- **Verdachte registersleutels** - sommige malware slaat zijn informatie op in het Windows register, om ervoor te zorgen dat deze informatie wordt geladen na het opstarten of om het effect ervan op het besturingssysteem te vergroten.

11.7.5. 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](#).



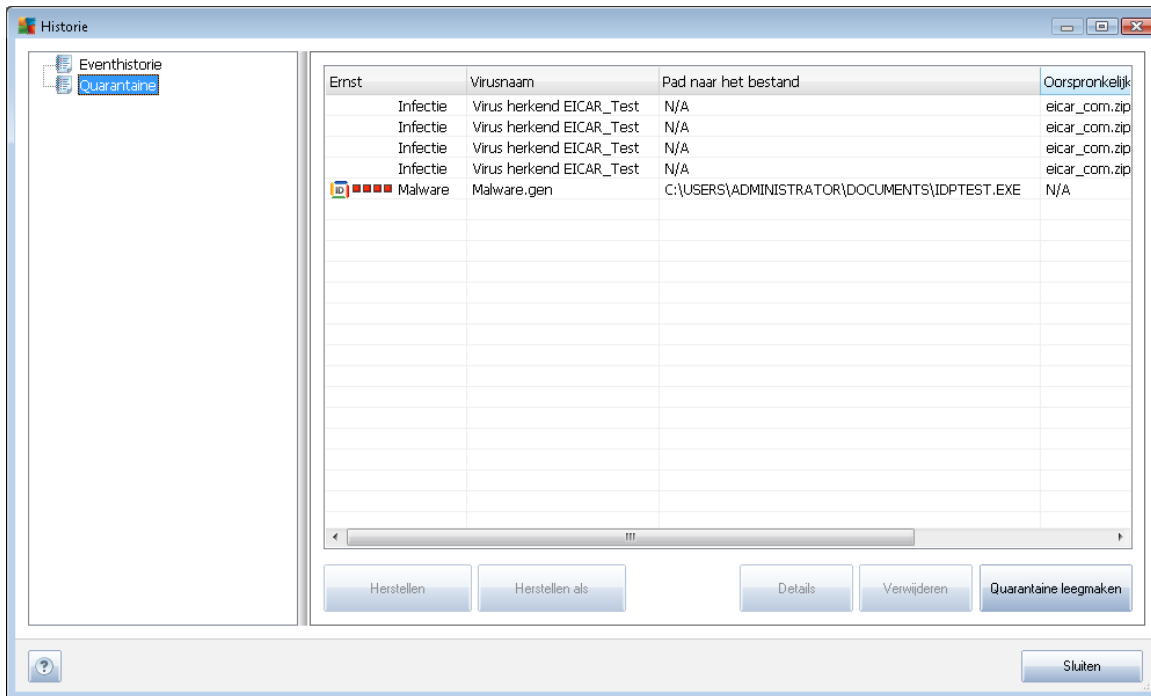
11.7.6. Tabblad Informatie

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

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

- **Runtime-gecomprimeerd** - het bestand is gecomprimeerd met een van de minder gangbare runtime-compressieprogramma's, wat kan duiden op een poging een scan van het bestand te ontwijken. Niet elk incident dat als zodanig wordt gerapporteerd, betreft ook daadwerkelijk een virus.
- **Runtime-gecomprimeerd recursief** - vergelijkbaar met bovenstaande, maar komt minder voor bij gangbare software. Dergelijke bestanden zijn verdacht en verwijdering of verzending voor analyse moet worden overwogen.
- **Met een wachtwoord beschermde documenten of archieven** - bestanden die zijn beveiligd met een wachtwoord kunnen door AVG niet worden gescand (*en in het algemeen niet met anti-malwareprogramma's*).
- **Document met macro's** - het gerapporteerde document bevat macro's die kwaadaardig kunnen zijn.
- **Verborgene extensies** - bestanden met verborgen extensies kunnen op het oog bijvoorbeeld afbeeldingsbestanden lijken te zijn, terwijl het in werkelijkheid uitvoerbare bestanden zijn (*bijvoorbeeld picture.jpg.exe*). De tweede extensie is in Windows standaard niet zichtbaar en AVG rapporteert dergelijke bestanden om te voorkomen dat ze per ongeluk worden geopend.
- **Onjuist bestandspad** - als een belangrijk systeembestand wordt uitgevoerd vanuit een andere map dan de standaardmap (*het bestand winlogon.exe wordt bijvoorbeeld uitgevoerd vanuit een andere map dan de map Windows*), wordt dat door AVG gemeld. In sommige gevallen gebruiken virussen de namen van standaardprocessen om minder opvallend aanwezig te zijn in het systeem.
- **Vergrendeld bestand** - het gerapporteerde bestand is vergrendeld en kan dus niet worden gescand door AVG. Dat betekent meestal dat een bestand voortdurend wordt gebruikt door het systeem (*bijvoorbeeld het wisselbestand*).

11.8. 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 hoofdoel 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 Internet Security 2011** 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

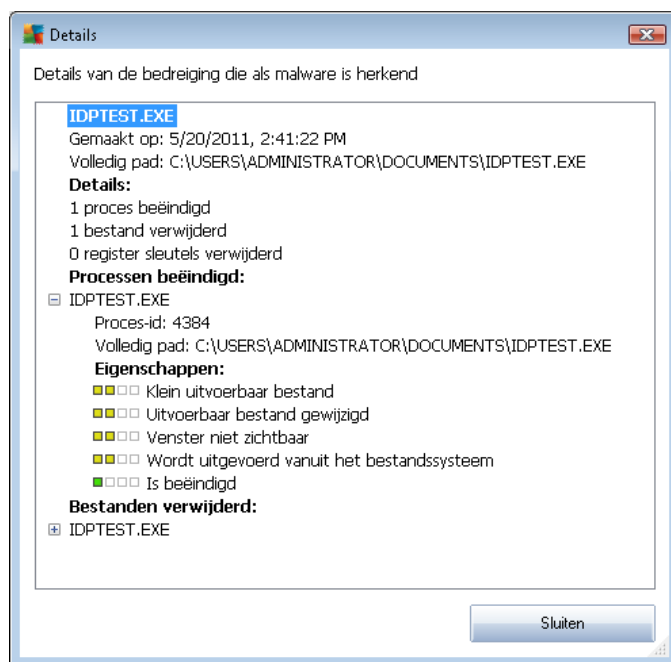
het diagram zijn gelabeld met de standaardnaam die werd gegeven door AVG tijdens de scanprocedure. Als het object een specifieke, oorspronkelijke naam had die bekend is, (bijvoorbeeld een naam van een e-mailbijlage die geen relatie heeft tot de feitelijke inhoud van de bijlage), wordt de naam weergegeven 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).



12. AVG Updates

Het is van cruciaal belang om uw AVG up-to-date te houden zodat alle nieuw ontdekte virussen zo snel mogelijk gedetecteerd kunnen worden.

Het is raadzaam om minstens eenmaal per dag te controleren of er nieuwe updates zijn, omdat AVG-updates niet volgens een bepaald schema worden uitgebracht, maar in reactie op het aantal bedreigingen en de ernst daarvan. Alleen op die manier bent u er zeker van dat **AVG Internet Security 2011** voortdurend up-to-date is.

12.1. Updateniveaus

AVG kent drie updateniveaus die u kunt selecteren:

- **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.

Bij het [plannen van een update](#), kunt u selecteren op welk prioriteitsniveau u wilt downloaden en updates wilt uitvoeren.

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

12.2. Soorten updates

Er zijn twee soorten updates te onderscheiden:

- **Een update op verzoek** is een onmiddellijke AVG-update die kan worden uitgevoerd zodra de noodzaak zich daartoe voordoet.
- **Geplande update** – U kunt in AVG ook een [updateplan instellen](#). De geplande update wordt vervolgens op basis van de ingestelde configuratie periodiek uitgevoerd. Wanneer er op de ingestelde locatie nieuwe updatebestanden beschikbaar zijn, worden deze rechtstreeks van internet of vanuit de netwerkmap gedownload. Als er geen nieuwe updates beschikbaar zijn, gebeurt er niets.

12.3. Updateprocedure

De updateprocedure kan als dat nodig is, onmiddellijk worden uitgevoerd als u op de snelkoppeling **Nu bijwerken** klikt. De koppeling is altijd actief in alle dialoogvensters van de [AVG gebruikersinterface](#). Het blijft echter raadzaam om regelmatig updates uit te voeren met behulp van het updateschema dat u kunt bewerken in het onderdeel [Updatebeheer](#).

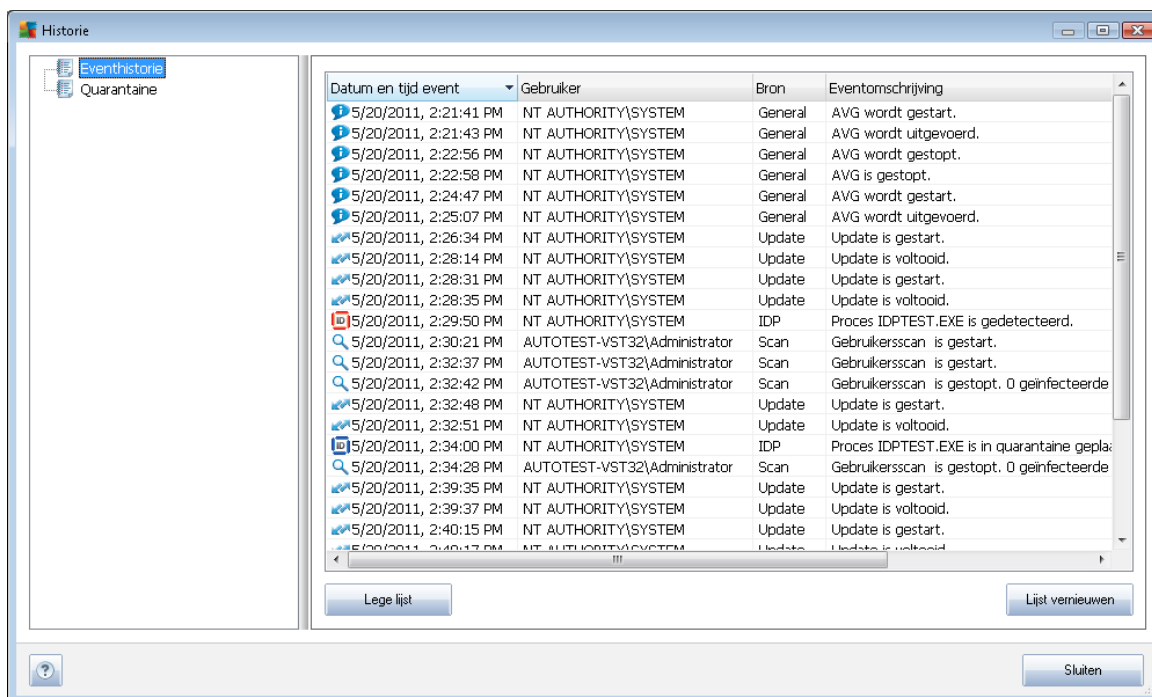
Als u de updateprocedure start, wordt eerst gecontroleerd of er nieuwe updates beschikbaar zijn. Zo ja, dan worden die gedownload en wordt het proces voor het bijwerken op gang gebracht. Tijdens het uitvoeren van de updateprocedure wordt het dialoogvenster **Update** geopend dat op grafische wijze de voortgang in beeld brengt en bovendien een overzicht geeft van de relevante statistische



parameters (grootte updatebestand, ontvangen gegevens, downloadsnelheid, verstreken tijd, ...).

Opmerking: Voorafgaand aan de start van de AVG-programma-update wordt een systeemherstelpunt gemaakt. Als de updateprocedure faalt en uw besturingssysteem crasht, kunt u uw besturingssysteem altijd herstellen in de oorspronkelijke configuratie vanaf dit punt. Deze optie is toegankelijk via Start / Alle programma's / Accessoires / Systeemprogramma's / Systeemherstel. Het aanbrengen van wijzigingen wordt alleen aanbevolen aan ervaren gebruikers!

13. 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 Internet Security 2011** zijn opgetreden. In het logboek **Historie worden de volgende gebeurtenistypen vastgelegd:**

- Informatie over updates van de AVG-toepassing
- Het begin, einde en onderbreking van een scan (*inclusief automatisch uitgevoerde scans*)
- 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 gebeurtenis** – het exacte moment dat de gebeurtenis plaatsvond
- **Gebruiker** – de gebruiker die de gebeurtenis heeft geïnitieerd
- **Bron** – het onderdeel of het deel van het systeem dat de aanleiding vormde voor het plaatsvinden van de gebeurtenis
- **Beschrijving gebeurtenis** – een korte samenvatting van wat er feitelijk gebeurde



Knoppen

- **Lijst legen** – alle items uit de lijst gebeurtenissen verwijderen
- **Lijst vernieuwen** – alle items in de lijst gebeurtenissen bijwerken



14. Veelgestelde vragen en technische ondersteuning

Mocht u problemen ondervinden met AVG, op zakelijk of technisch gebied, raadpleeg dan de sectie met [veelgestelde vragen\(FAQ\)](#) op de website van AVG (<http://www.avg.com/>).

Vindt u op die manier geen oplossing, neem dan via e-mail contact op met de technische ondersteuningsdienst. Gebruik daarvoor het contactformulier dat u kunt oproepen via het menu **Help / Online Help**.